Dell™ AppAssure™

Benutzerhandbuch

5.4.3

© 2014 Dell Inc.
ALLE RECHTE VORBEHALTEN.

Dieses Handbuch enthält urheberrechtlich geschützte Informationen. Die im vorliegenden Handbuch beschriebene Software unterliegt den Bedingungen der jeweiligen Softwarelizenz oder Geheimhaltungsvereinbarung. Die Software darf nur gemäß den Bedingungen der Vereinbarung benutzt oder kopiert werden. Ohne ausdrückliche schriftliche Erlaubnis von Dell Inc. darf diese Anleitung weder ganz noch teilweise zu einem anderen Zweck als dem persönlichen Gebrauch des Käufers vervielfältigt oder übertragen werden, unabhängig davon, auf welche Weise oder mit welchen Mitteln, elektronisch oder mechanisch, durch Fotokopieren oder Aufzeichnen, dies geschieht.

Die Informationen in diesem Dokument werden in Verbindung mit Dell-Produkten zur Verfügung gestellt. Durch dieses Dokument wird weder explizit noch implizit, durch Duldungsvollmacht oder auf andere Weise, eine Lizenz auf intellektuelle Eigentumsrechte erteilt, auch nicht in Verbindung mit dem Erwerb von Dell-Produkten. IN DEN ALLGEMEINEN GESCHÄFTSBEDINGUNGEN, DIE IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT AUFGEFÜHRT SIND, ÜBERNIMMT DELL KEINERLEI HAFTUNG UND SCHLIESST JEDE EXPLIZITE, IMPLIZITE ODER GESETZLICHE GEWÄHRLEISTUNG FÜR SEINE PRODUKTE AUS, INSBESONDERE DIE IMPLIZITE GEWÄHRLEISTUNG DER MARKTFÄHIGKEIT, DER EIGNUNG ZU EINEM BESTIMMTEN ZWECK UND DIE GEWÄHRLEISTUNG DER NICHTVERLETZUNG VON RECHTEN. UNTER KEINEN UMSTÄNDEN HAFTET DELL FÜR UNMITTELBARE, MITTELBARE ODER FOLGESCHÄDEN, SCHADENERSATZ, BESONDERE ODER KONKRETE SCHÄDEN (INSBESONDERE SCHÄDEN, DIE AUS ENTGANGENEN GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER DATENVERLUSTEN ENTSTEHEN), DIE SICH DURCH DIE NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS ERGEBEN, AUCH WENN DELL ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE. Dell übernimmt keine Garantie für die Richtigkeit oder Vollständigkeit der Inhalte dieses Dokuments und behält sich vor, jederzeit und ohne vorherige Ankündigung Änderungen an den Spezifikationen und Produktbeschreibungen vorzunehmen. Dell geht keinerlei Verpflichtung ein, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Bei Fragen zur möglichen Verwendung dieser Materialien wenden Sie sich an:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Informationen zu regionalen und internationalen Niederlassungen finden Sie auf unserer Website (software.dell.com).

Die Dell AppAssure 5-Software nutzt die Emit Mapper-DLL v. 1.0.0 (Dynamic Link Library), die im Rahmen der GNU Library General Public License (LGPL) Version 2.1, Februar 1999 lizenziert ist. Der Copyright-Hinweis von Emit Mapper lautet: „Copyright © 1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.“

Benutzer können den vollständigen Text der LGPL-Lizenz unter http://www.software.dell.com/legal/license-agreements.aspx als Lizenzvereinbarung eines externen Anbieters anzeigen. Den Quellcode von Emit Mapper finden Sie unter http://opensource.dell.com/.

Marken

Dell, das Dell-Logo und AppAssure sind Marken von Dell Inc. und/oder zugehörigen Tochtergesellschaften. Andere in diesem Dokument verwendete Marken und Handelsnamen beziehen sich auf die Unternehmen, die Rechteinhaber der Marken und Handelsnamen sind, oder auf deren Produkte. Dell beansprucht keinerlei Eigentumsrechte an Marken und Markennamen außer den eigenen Marken und Markennamen.

Legende

△ **VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.**

⚠ **WARNUNG: Das Symbol WARNUNG weist auf mögliche Personen- oder Sachschäden oder Schäden mit Todesfolge hin.**

ⓘ **WICHTIG**, **HINWEIS**, **TIPP**, **MOBIL** oder **VIDEO:** Ein Informationssymbol weist auf Begleitinformationen hin.

Dell AppAssureBenutzerhandbuch
Aktualisiert: Dezember 2014
Softwareversion: 5.4.3

Inhalt

Einführung in AppAssure 11
Informationen zu AppAssure 11
Zentrale Technologien von AppAssure 12
Live Recovery 12
Verified Recovery 12
Universal Recovery 12
True Global Deduplication 12
Produktfunktionen von AppAssure 13
Repository 13
True Global Deduplication 13
Verschlüsselung 15
Replikation 15
Recovery-as-a-Service (RaaS) 16
Aufbewahrung und Archivierung 17
Virtualisierung und die Cloud 17
Benachrichtigungen und Ereignisverwaltung 19
Lizenzportal 19
Webkonsole 19
Dienstverwaltungs-APIs 19
White-Labeling 19
AppAssure-Assistenten 20

Arbeiten mit dem AppAssure Core 22
Öffnen der AppAssure Core Console 23
Navigieren zur AppAssure Core Console. 23
Anzeigen und Verwalten geschützter Maschinen 25
Informationen zur Registerkarte „Zusammenfassung“ 26
Informationen zur Kurzanleitung 27
Starten der Kurzanleitung 29
Ausblenden der Kurzanleitung 29
Informationen zu benutzerdefinierten Gruppen 30
Erstellen von benutzerdefinierten Gruppen 31
Ändern der Namen von benutzerdefinierten Gruppen 31
Entfernen von benutzerdefinierten Gruppen 32
Durchführen von Gruppenaktionen 32
Anzeigen aller Maschinen in einer benutzerdefinierten Gruppe auf einer Seite 33
Anleitung zum Konfigurieren des AppAssure Core 33
Verwalten von Lizenzen 34
Ändern eines Lizenzschlüssels 35
Verbindungsaufbau zum Dell Software-Lizenzportal-Server 35
Verwalten der AppAssure Core-Einstellungen 35
Ändern des Core-Anzeigenamens 36
Konfigurieren von Updateeinstellungen 36
Konfigurieren nächtlicher Jobs für den Core 37

Aktivieren einer nächtlichen Bereitstellungsprüfung 37
Einstellen der Uhrzeit für nächtliche Jobs 38
Ändern der Einstellungen für die Übertragungswarteschlange 38
Anpassen der Client-Zeitlimiteinstellungen 39
Grundlegende Informationen zur Größe des Deduplizierungscache sowie zu Speicherorten 39
Konfigurieren von Deduplizierungscache-Einstellungen 40
Ändern der AppAssureEngine-Einstellungen 41
Ändern von Bereitstellungseinstellungen 42
Ändern der Datenbankverbindungseinstellungen 43
Informationen zu Repositorys 43
Anleitung für die Verwaltung eines Repositorys 44
Erstellen eines Repositorys 45
Anzeigen von Details für ein Repository 47
Ändern der Repository-Einstellungen 48
Hinzufügen eines Speicherorts zu einem vorhandenen Repository 49
Überprüfen eines Repositorys. 52
Löschen eines Repositorys 52
Informationen zum Integritätsprüfjob für Repositorys 52
Ausführen des Integritätsprüfjobs für ein Repository 53
Verwalten der Sicherheit 54
Hinzufügen eines Verschlüsselungsschlüssels 54
Bearbeiten eines Verschlüsselungsschlüssels 55
Ändern der Passphrase für einen Verschlüsselungsschlüssel 56
Importieren eines Verschlüsselungsschlüssels 56
Exportieren eines Verschlüsselungsschlüssels 56
Entfernen eines Verschlüsselungsschlüssels 57
Verwalten von Cloud-Konten 57
Hinzufügen eines Cloud-Kontos 57
Bearbeiten eines Cloud-Kontos 58
Konfigurieren von Cloud-Kontoeinstellungen 59
Entfernen eines Cloud-Kontos 59
Informationen zur Replikation 60
Informationen zum Seeding 62
Informationen zu Failover und Failback in AppAssure 63
Informationen zu Replikation und verschlüsselten Wiederherstellungspunkten 63
Informationen zu Aufbewahrungsrichtlinien für die Replikation 63
Überlegungen zur Übertragungsleistung für Replikationsdaten 64
Anleitung für die Einrichtung der Replikation 65
Replikation auf einen selbstverwalteten Ziel-Core 65
Replikation auf den Ziel-Core eines externen Anbieters 69
Senden einer Replikationsanforderung an einen externen Dienstanbieter 69
Überprüfen einer Replikationsanforderung von einem Kunden 72
Genehmigen einer Replikationsanforderung 72
Ablehnen einer Replikationsanforderung 73
Ignorieren einer Replikationsanforderung von einem Kunden 73
Hinzufügen einer Maschine zu einer bestehenden Replikation 74

Konsumieren des Seed-Laufwerks auf einem Ziel-Core 76
Entfernen eines ausstehenden Seed-Laufwerks 77
Verwalten der Replikationseinstellungen 78
Planen der Replikation 78
Überwachen der Replikation 79
Anhalten und Fortsetzen der Replikation 81
Erzwingen der Replikation 81
Verwalten der Einstellungen für die ausgehende Replikation 81
Ändern der Ziel-Core-Einstellungen 82
Festlegen der Replikationspriorität für einen Agenten 82
Aufheben der Replikation 83
Entfernen eines Agenten aus der Replikation auf dem Quell-Core 83
Entfernen eines Agenten auf dem Ziel-Core 83
Entfernen eines Ziel-Core aus der Replikation 83
Entfernen eines Quell-Core aus der Replikation 84
Wiederherstellen von replizierten Daten 84
Anleitung für Failover und Failback 84
Einrichten einer Umgebung für Failover 85
Durchführen eines Failovers auf dem Ziel-Core 85
Durchführen eines Failbacks 86
Verwalten von Ereignissen 87
Konfigurieren von Benachrichtigungsgruppen 87
Konfigurieren eines E-Mail-Servers 90
Konfigurieren einer E-Mail-Benachrichtigungsvorlage 91
Konfigurieren der Reduzierung der Wiederholungen 91
Konfigurieren der Ereignisaufbewahrung 92
Verwalten der Wiederherstellung 92
Informationen zu Systeminformationen 92
Anzeigen von Systeminformationen 92
Herunterladen von Installationsprogrammen 93
Informationen zum Agent Installer 93
Herunterladen des Agent Installers 93
Informationen zum Local Mount Utility 93
So laden Sie das Local Mount Utility herunter und installieren Sie es 94
Hinzufügen eines Core zum Local Mount Utility 95
Bereitstellen eines Wiederherstellungspunkts mit dem Local Mount Utility 96
Untersuchen eines bereitgestellten Wiederherstellungspunktes mit dem Local Mount Utility 97
Aufheben der Bereitstellung eines Wiederherstellungspunkts mit dem Local Mount Utility 97
Informationen zum Taskleistenmenü des Local Mount Utility 98
Verwenden der AppAssure Core- und Agent-Optionen 98
Verwalten von Aufbewahrungsrichtlinien 99
Anleitung für die Archivierung in einer Cloud 99
Grundlegende Informationen zu Archiven 99
Erstellen eines Archivs 100
Festlegen einer geplanten Archivierung 101

Deaktivieren oder Aktivieren einer geplanten Archivierung 103
Bearbeiten einer geplanten Archivierung 104
Überprüfen eines Archivs 105
Importieren eines Archivs 106
Verwalten von SQL-Anfügbarkeit und Protokollkürzung 107
Konfigurieren der SQL-Anfügbarkeitseinstellungen 108
Konfigurieren von nächtlichen SQL-Anfügbarkeitsprüfungen und Protokollkürzungen für alle geschützten Maschinen 109
Verwalten von Bereitstellbarkeitsprüfungen und Protokollkürzung für Exchange-Datenbanken 109
Konfigurieren von nächtlichen Prüfsummenprüfungen und Protokollkürzungen für Exchange-Datenbanken 110
Statusanzeigen für Wiederherstellungspunkte 110

Schützen von Arbeitsstationen und Servern 112
Informationen zum Schützen von Arbeitsstationen und Servern 113
Einschränkungen bei der Unterstützung dynamischer Volumes und Basis-Volumes . . 113
Informationen zu Schutzzeitplänen 113
Schützen einer Maschine 114
Erstellen benutzerdefinierter Schutzzeitpläne 119
Ändern von Schutzzeitplänen 120
Verwalten von Exchange- und SQL Server-Maschinen 122
Anpassen der nächtlichen Jobs für eine geschützte Maschine 125
Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion 126
Konfigurieren von Maschineneinstellungen 128
Anzeigen und Ändern von Konfigurationseinstellungen 128
Anzeigen von Systeminformationen für eine Maschine 129
Konfigurieren von Benachrichtigungsgruppen für Systemereignisse 130
Bearbeiten von Benachrichtigungsgruppen für Systemereignisse 132
Konfigurieren von Standardeinstellungen für die Aufbewahrungsrichtlinie des Core . 134
Anpassen der Aufbewahrungsrichtlinieneinstellungen für einen Agenten 136
Anzeigen von Lizenzinformationen 138
Ändern der Übertragungseinstellungen 139
Anzeigen von Systemdiagnoseinformationen 141
Anzeigen von Maschinenprotokollen 141
Hochladen von Maschinenprotokollen 142
Verwalten von Core-Jobeinstellungen 142
Bearbeiten von Core-Jobeinstellungen 142
Hinzufügen von Core-Jobs 142
Bereitstellen eines Agenten (Push-Installation) 144
Verwalten von Maschinen 144
Entfernen einer Maschine 145
Abbrechen von Vorgängen für eine Maschine 145
Anzeigen des Maschinenstatus und anderen Details 145
Verwalten mehrerer Maschinen 146
Bereitstellung auf mehreren Maschinen 147
Bereitstellung auf Maschinen in einer Active Directory-Domäne 147
Bereitstellung auf Maschinen auf einem virtuellen VMware vCenter/ESX(i)-Host . . . 149

Bereitstellung auf Maschinen auf beliebigen anderen Hosts 150
Überprüfen der Bereitstellung auf mehreren Maschinen 151
Schützen mehrerer Maschinen 151
Überwachen des Schutzes von mehreren Maschinen 156
Verwalten von Snapshots und Wiederherstellungspunkten 156
Anzeigen von Wiederherstellungspunkten 156
Anzeigen eines bestimmten Wiederherstellungspunkts 157
Bereitstellen eines Wiederherstellungspunktes für eine Windows-Maschine 159
Aufheben der Bereitstellung ausgewählter Wiederherstellungspunkte 160
Aufheben der Bereitstellung aller Wiederherstellungspunkte 160
Bereitstellen eines Wiederherstellungspunkt-Volumes für eine Linux-Maschine 161
Aufheben der Bereitstellung eines Wiederherstellungspunkts auf einer Linux-Maschine . 162
Entfernen von Wiederherstellungspunkten 163
Löschen einer verwaisten Wiederherstellungspunktkette 163
Erzwingen eines Snapshots 164
Verwalten von SQL- und Exchange-Servern 164
Festlegen der Anmeldeinformationen für Exchange-Server 165
Festlegen der Anmeldeinformationen für SQL-Server 165
Informationen zum Wiederherstellen von Daten aus Wiederherstellungspunkten 166
Wiederherstellen von Volumes aus einem Wiederherstellungspunkt 167
Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile 170
Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer 171
Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer und Beibehalten der Berechtigungen 172
Information zum Exportieren geschützter Daten von Windows-Maschinen in virtuelle Maschinen 172
Verwalten von Exporten 173
Exportieren von Daten aus einer Windows-Maschine in eine virtuelle Maschine 175
Exportieren von Windows-Daten mit ESXi-Export 176
Exportieren von Windows-Daten mit VMware Workstation-Export 178
Exportieren von Windows-Daten mit Hyper-V-Export 182
Exportieren von Windows-Daten nach VirtualBox 186
Exportieren von Sicherungsinformationen aus einer Linux-Maschine in eine virtuelle Maschine 189
Durchführen eines einmaligen VirtualBox-Exports 189
Durchführen eines kontinuierlichen VirtualBox-Exports (Virtual Standby) 190
Grundlegende Informationen zur BMR-Wiederherstellung 191
Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen 193
Voraussetzungen für eine BMR-Wiederherstellung für Windows-Maschinen 194
Verwalten eines Windows-Start-Image 194
Erstellen eines ISO-Image für eine Start-CD für Windows 195
Festlegen der Parameter für das ISO-Image der Start-CD 195
Benennen der Start-CD-Datei und Festlegen des Pfads 195
Erstellen von Verbindungen 196
Angeben einer Wiederherstellungsumgebung 196
Injizieren von Treibern in eine Start-CD 197
Erstellen des ISO-Image für die Start-CD 197

Anzeigen des Fortschritts der ISO-Image-Erstellung 198
Zugreifen auf das ISO-Image 198
Übertragen des ISO-Image der Start-CD auf Datenträger 198
Laden der Start-CD und Starten der Zielmaschine 198
Verwalten eines Windows-Start-Image und Starten einer BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine 199
Starten einer BMR-Wiederherstellung für Linux 202
Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung 203
Zuordnen von Volumes für eine BMR-Wiederherstellung 204
Laden von Treibern mit der Universal Recovery Console 205
Injizieren von Treibern auf dem Zielserver 206
Überprüfen einer BMR-Wiederherstellung 206
Anzeigen des Fortschritts der Wiederherstellung 207
Starten eines wiederhergestellten Zielservers 207
Beheben von Universal Recovery Console-Verbindungsproblemen 207
Reparieren von Startproblemen 208
Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen 208
Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen 209
Verwalten eines Linux-Start-Image 210
Herunterladen eines ISO-Start-Image für Linux 210
Übertragen desLive DVD ISO-Image auf Datenträger 211
Laden der Live DVD und Starten der Zielmaschine 211
Verwalten von Linux-Partitionen 212
Erstellen von Partitionen auf dem Ziellaufwerk 212
Formatieren von Partitionen auf dem Ziellaufwerk 213
Mounten von Partitionen über die Befehlszeile 214
Starten einer BMR-Wiederherstellung für Linux 215
Starten des Dienstprogramms „Screen“ 215
Starten einer BMR-Wiederherstellung für eine Linux-Maschine über die Befehlszeile 216
Überprüfen der BMR-Wiederherstellung über die Befehlszeile 218
Durchführen einer Dateisystemprüfung für das wiederhergestellte Volume 218
Erstellen startfähiger Partitionen auf der wiederhergestellten Linux-Maschine über die Befehlszeile 219
Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen 222
Anzeigen von Aufgaben 222
Anzeigen von Benachrichtigungen 223
Anzeigen aller Ereignisse 224

Schützen von Server-Clustern 225
Informationen zum Schützen von Server-Clustern in AppAssure 225
Unterstützte Anwendungen und Cluster-Typen 226
Begrenzte Unterstützung für freigegebene Clustervolumes. 226
Schützen eines Clusters 227
Schützen von Knoten in einem Cluster 228
Ändern der Einstellungen für Cluster-Knoten 229
Anleitung zum Konfigurieren von Cluster-Einstellungen 230
Ändern der Cluster-Einstellungen 230

Konfigurieren der Benachrichtigungen für Cluster-Ereignisse 231
Bearbeiten der Cluster-Aufbewahrungsrichtlinie 232
Ändern der Cluster-Schutzzeitpläne 233
Ändern der Cluster-Übertragungseinstellungen 233
Konvertieren eines geschützten Cluster-Knotens in einen Agenten 233
Anzeigen von Informationen für Server-Cluster 234
Anzeigen von Cluster-Systeminformationen 234
Anzeigen von Cluster-Aufgaben, -Ereignissen und -Warnungen 234
Anzeigen von zusammenfassenden Informationen 235
Verwenden von Cluster-Wiederherstellungspunkten 235
Verwalten von Snapshots für einen Cluster 236
Erzwingen der Snapshot-Erstellung für einen Cluster 236
Anhalten und Fortsetzen der Erstellung von Cluster-Snapshots 236
Aufheben der Bereitstellung lokaler Wiederherstellungspunkte 237
Durchführen einer Wiederherstellung für Cluster und Cluster-Knoten 237
Durchführen einer Wiederherstellung für CCR- (Exchange) und DAG-Cluster 237
Durchführen einer Wiederherstellung für SCC-Cluster (Exchange, SQL) 238
Replizieren von Cluster-Daten 238
Aufheben des Clusters-Schutzes 238
Aufheben des Schutzes von Cluster-Knoten 239
Aufheben des Schutzes aller Knoten in einem Cluster 239
Anzeigen eines Cluster- oder Knotenberichts 239

Berichterstellung 241
Informationen zu Berichten 241
Informationen zur Symbolleiste für Berichte 242
Informationen zu Complianceberichten 242
Informationen zu Fehlerberichten 243
Informationen zu Zusammenfassungsberichten 243
Repositoryübersicht 243
Agentenübersicht 244
Erstellen eines Berichts für einen Core oder Agenten 244
Informationen zu Berichten für Cores in der Central Management Console 245
Erstellen eines Berichts in der Central Management Console 245

Skripterstellung 246
PowerShell Scripting in AppAssure 246
Voraussetzungen für die Erstellung von PowerShell-Skripts 247
powershell.exe.config 247
Testen von PowerShell-Skripts 247
Eingabeparameter für PowerShell-Skripts 247
Beispiele für PowerShell-Skripts 258
PreTransferScript.ps1 259
PostTransferScript.ps1 259
PreExportScript.ps1 260
PostExportScript.ps1 260
PreNightlyJobScript.ps1 261

PostNightlyJobScript.ps1 263
Informationen zum Erstellen von Bourne Shell-Skripts in AppAssure 266
Voraussetzungen für Bourne Shell-Skripts 266
Testen von Bourne Shell-Skripts 266
Eingabeparameter für Bourne Shell-Skripts 266
Beispiele für Bourne Shell-Skripts 268
PreTransferScript.sh 268
PostTransferScript.sh 269
PostExportScript.sh 269

Glossar 270

Informationen zu Dell 276
Kontakt zu Dell 276
Technische Supportressourcen 276

1

Einführung in AppAssure

Dieses Kapitel bietet eine Einführung in sowie einen Überblick über Dell AppAssure. Es umfasst eine Beschreibung der Merkmale, Funktionen sowie der Architektur. Die folgenden Themen werden behandelt:

- Informationen zu AppAssure
- Zentrale Technologien von AppAssure
- Produktfunktionen von AppAssure

Informationen zu AppAssure

AppAssure setzt neue Standards beim einheitlichen Datenschutz, indem Sicherung, Replikation und

Wiederherstellung in einer Lösung kombiniert werden, die als extrem schnelle und zuverlässige Sicherungslösung zum Schutz virtueller Maschinen (VM) sowie physischer Maschinen und Cloud-Umgebungen konzipiert wurde.

AppAssure kombiniert Sicherung und Replikation in einem integrierten und einheitlichen Datenschutzprodukt, das außerdem durch Anwendungserkennung für eine zuverlässige Wiederherstellung von Anwendungsdaten aus Ihren Sicherungen sorgt. AppAssure ist auf der neuen, zum Patent angemeldeten True Scale-Architektur aufgebaut, die dank offensiver und extrem kurzer Wiederherstellungsdauer (RTO, Recovery Time Objective) sowie durch kurze zeitliche Abstände zwischen Wiederherstellungspunkten (RPO, Recovery Point Objective) die schnellste Sicherungsleistung bietet.

In AppAssure sind mehrere einzigartige, innovative und bahnbrechende Technologien zusammengefasst:

- Live Recovery
- Verified Recovery
- Universal Recovery
- True Global Deduplication

Diese Technologien sind mit zuverlässiger Integration für die Cloud-Notfallwiederherstellung ausgestattet und ermöglichen eine schnelle und verlässliche Wiederherstellung. Mit seinem skalierbaren Objektspeicher und dank der integrierten globalen Deduplizierung, Komprimierung, Verschlüsselung sowie Replikation in privaten oder öffentlichen Cloud-Infrastrukturen kann AppAssure als einzige Lösung sogar bis zu Petabyte an Daten schnell verarbeiten. Innerhalb von Minuten können Serveranwendungen und Daten für Datenaufbewahrung sowie Compliance wiederhergestellt werden.

Die heute verfügbaren älteren Sicherungstools und VM-Sicherungstools der ersten Generation sind ineffizient und ineffektiv. Zum einen können diese veralteten Sicherungstools keine größeren Datenmengen verarbeiten, zum anderen bieten sie nicht die Leistung und Zuverlässigkeit, die zum Schutz geschäftskritischer Anwendungen nötig sind. Bei komplexen und gemischten IT-Umgebungen entstehen dadurch administrative Herausforderungen für die IT-Mitarbeiter sowie Sicherheitsrisiken für die Systemdaten.

AppAssure geht diese Komplexität und Ineffizienz durch unsere Core-Technologie und Unterstützung von Umgebungen mit mehreren Hypervisoren an, z. B. Umgebungen auf Basis von VMware vSphere und Microsoft Hyper-V, die sowohl private als auch öffentliche Clouds umfassen. Mit AppAssure können Sie jedoch nicht nur diese technologischen Fortschritte nutzen, sondern auch die Kosten der IT-Verwaltung und Speicherung drastisch senken.

Zentrale Technologien von AppAssure

In den folgenden Abschnitten werden die zentralen Technologien von AppAssure ausführlich beschrieben.

Live Recovery

Live Recovery ist eine Technologie zur Sofortwiederherstellung für VMs oder Server, die nahezu ununterbrochenen Zugriff auf Daten-Volumes auf virtuellen oder physischen Servern ermöglicht. Mit dieser Technologie können Sie ein komplettes Volume in extrem kurzer RTO-Zeit und RPO-Zeiten von wenigen Minuten wiederherstellen.

Die Sicherungs- und Replikationstechnologie von AppAssure erstellt simultane Snapshots von mehreren VMs oder Servern und ermöglicht so nahezu sofortigen Daten- und Systemschutz. Sie können den Server direkt aus der Sicherungsdatei weiter verwenden, ohne eine vollständige Wiederherstellung auf dem Produktionsspeicher abwarten zu müssen. Dadurch bleibt die Produktivität der Benutzer erhalten und die IT-Abteilungen können die Zahl der Wiederherstellungsfenster reduzieren, um die immer strengeren SLAs hinsichtlich RTO und RPO erfüllen zu können.

Verified Recovery

Mit Verified Recovery können Sie automatisierte Wiederherstellungstests durchführen und Sicherungen überprüfen. Recovery Assure unterstützt u. a. Dateisysteme, Microsoft Exchange Server 2007, 2010 und 2013 sowie Microsoft SQL Server 2005, 2008, 2008 R2, 2012 und 2014. Verified Recovery ermöglicht die Wiederherstellung von Anwendungen und Sicherungen in virtuellen und physischen Umgebungen und verfügt über einen umfassenden Algorithmus für die Integritätsprüfung, der auf 256-Bit SHA-Schlüsseln basiert, mit denen bei Archivierungs-, Replikations- und Datenseedingvorgängen die Richtigkeit aller Datenträgerblöcke in der Sicherung überprüft wird. Dadurch kann die Beschädigung von Daten rechtzeitig erkannt werden und es wird verhindert, dass beschädigte Datenblöcke beibehalten oder während der Sicherungsvorgänge übertragen werden.

Universal Recovery

Die Universal Recovery-Technologie bietet uneingeschränkte Flexibilität bei der Wiederherstellung von Maschinen. Sie können Ihre Sicherungen auf folgenden Umgebungen wiederherstellen: von physischen auf virtuellen, von virtuellen auf virtuellen, von virtuellen auf physischen oder von physischen auf physischen. Darüber hinaus können Sie eine BMR-Wiederherstellung (Bare Metal Restore) auf anderer Hardware, z. B. P2V, V2V, V2P, P2P, P2C, V2C, C2P und C2V, durchführen.

Zudem beschleunigt diese Technologie plattformübergreifende Verschiebungen zwischen virtuellen Maschinen, zum Beispiel von VMware zu Hyper-V bzw. von Hyper-V zu VMware. Sie ermöglicht die Wiederherstellung auf Anwendungs-, Element- und Objektebene von einzelnen Dateien, Ordnern, E-Mails, Kalenderelementen, Datenbanken und Anwendungen. Mit AppAssure können Sie außerdem physische oder virtuelle Daten aus der Cloud wiederherstellen sowie in die Cloud exportieren.

True Global Deduplication

AppAssure umfasst True Global Deduplication, ein Verfahren, mit dem die Kapazitätsanforderungen der physischen Datenträger erheblich reduziert werden können. Dabei werden Speicherplatzeinsparungsverhältnisse von über 50:1 erreicht und gleichzeitig die Datenspeicheranforderungen erfüllt. Die Inline-Komprimierung und -Deduplizierung von True Scale auf Blockebene mit Verbindungsgeschwindigkeit und die vordefinierte

Integritätsprüfung verhindern, dass die Sicherungs- und Archivierungsvorgänge durch Datenbeschädigungen beeinträchtigt werden.

Produktfunktionen von AppAssure

AppAssure umfasst die folgenden Komponenten und Funktionen, mit denen Sie alle Aspekte zum Schutz und zur Wiederherstellung von kritischen Daten verwalten können. Dazu gehören:

- Repository
- True Global Deduplication
- Verschlüsselung
- Replikation
- Recovery-as-a-Service (RaaS)
- Aufbewahrung und Archivierung
- Virtualisierung und die Cloud
- Benachrichtigungen und Ereignisverwaltung
- Lizenzportal
- Webkonsole
- Dienstverwaltungs-APIs
- White-Labeling
- AppAssure-Assistenten

Repository

Das AppAssure-Repository verwendet einen Volume-Manager zur Deduplizierung (DVM), um einen Volume-Manager zu implementieren, der Unterstützung für mehrere Volumes bietet, die sich auf verschiedenen Speichertechnologien befinden können, z. B. Storage Area Network (SAN), direkt angeschlossener Speicher, Network Attached Storage (NAS) oder Cloud-Speicher. Jedes Volume besteht aus einem skalierbaren Objektspeicher mit Deduplizierung. Der skalierbare Objektspeicher verhält sich wie ein datensatzbasiertes Dateisystem, bei dem die Einheit der Speicherzuweisung ein Datenblock mit fester Größe ist, der Datensatz genannt wird. Mit dieser Architektur können Sie Komprimierung und Deduplizierung auf Blockebene konfigurieren. Rollup-Vorgänge werden von datenträgerintensiven Vorgängen auf Metadatenvorgänge reduziert, da beim Rollup keine Daten mehr verschoben werden, sondern nur noch die Datensätze.

Der DVM kann mehrere Objektspeicher in einem Volume kombinieren. Diese können durch Erstellen zusätzlicher Dateisysteme erweitert werden. Die Objektspeicherdateien werden vorab zugewiesen und können bei Bedarf hinzugefügt werden, falls sich die Speicheranforderungen ändern. In einem einzigen AppAssure Core können bis zu 255 unabhängige Repositorys erstellt werden. Zusätzlich kann ein Repository durch Hinzufügen neuer Dateierweiterungen weiter vergrößert werden. Ein erweitertes Repository kann bis zu 4.096 Erweiterungen enthalten, die verschiedene Speichertechnologien umfassen. Die Maximalgröße eines Repositorys beträgt 32 Exabyte. In einem Core können sich mehrere Repositorys befinden.

True Global Deduplication

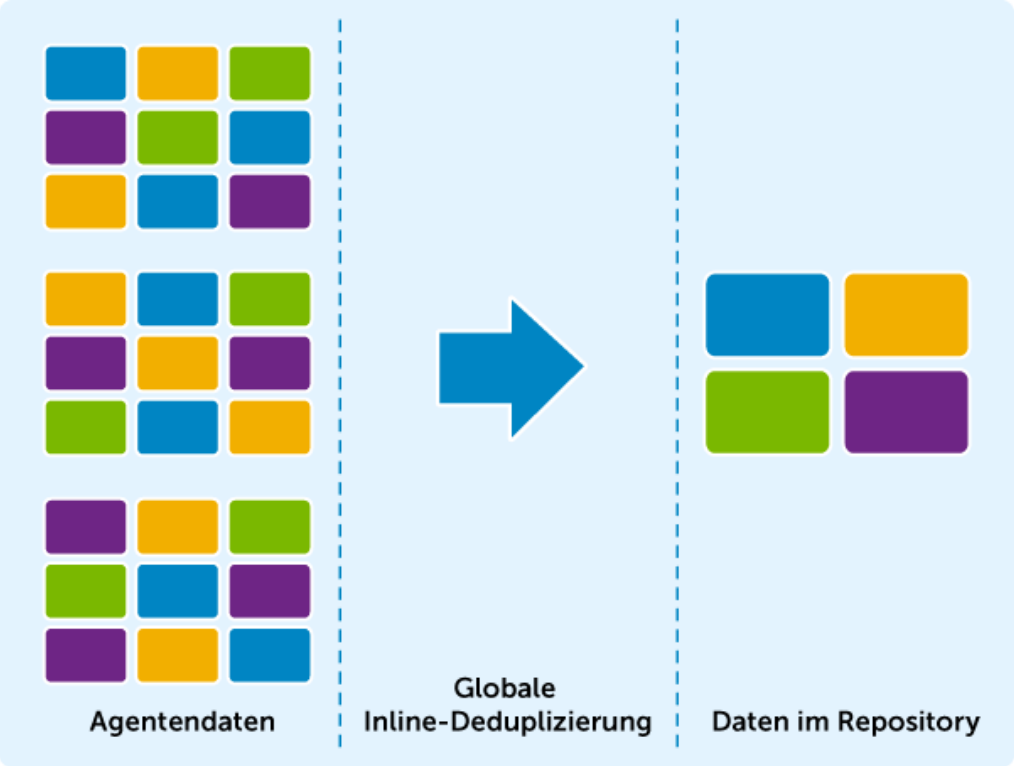
Mit True Global Deduplication kann der erforderliche Speicher für Sicherungen durch Löschen redundanter oder doppelter Daten effektiv reduziert werden. Da im Repository nur eine einzige Instanz der Daten aus mehreren Sicherungen gespeichert wird, ist die Deduplizierung äußerst effektiv. Die redundanten Daten werden zwar

gespeichert, jedoch nicht physisch abgelegt, sondern einfach durch einen Zeiger auf die jeweilige einmalige Dateninstanz im Repository ersetzt.

Bei herkömmlichen Sicherungsanwendungen werden wöchentlich iterative Vollsicherungen durchgeführt. AppAssure hingegen führt fortlaufende inkrementelle Sicherungen der Maschine auf Blockebene durch. Zusammen mit der Datendeduplizierung hilft dieser Ansatz einer fortlaufenden inkrementellen Sicherung dabei, das Gesamtvolumen der auf dem Datenträger gespeicherten Daten erheblich zu reduzieren.

Das typische Datenträgerlayout eines Servers umfasst Betriebssystem, Anwendung und Daten. In den meisten Umgebungen nutzen die Administratoren für eine effektive Bereitstellung und Verwaltung oftmals eine gemeinsame Konfiguration des Server- und Desktopbetriebssystems für mehrere Systeme. Wenn AppAssure eine Sicherung auf Blockebene für mehrere Maschinen gleichzeitig durchführt, erhalten Sie einen detaillierten Überblick über die Inhalte, die gesichert bzw. nicht gesichert werden (unabhängig von der Quelle). Zu diesen Daten gehören das Betriebssystem, die Anwendungen und die Anwendungsdaten in der Umgebung.

Abbildung 1. True Global Deduplication



AppAssure führt zielbasierte Inline-Datendeduplizierungen durch. Bei dieser Methode werden die Snapshot-Daten vor ihrer Deduplizierung an den Core übertragen. Bei der Inline-Datendeduplizierung werden – vereinfacht ausgedrückt – die Daten dedupliziert, bevor sie an den Datenträger übergeben werden. Dieses Verfahren unterscheidet sich grundlegend von der Deduplizierung auf der Quelle, bei der die Daten an der Quelle dedupliziert werden, bevor sie zur Speicherung auf das Ziel übertragen werden, und auch von der Deduplizierung nach der Verarbeitung, bei der die Daten als Rohdaten an das Ziel gesendet werden, wo sie nach der Übergabe an den Datenträger analysiert und dedupliziert werden. Bei der Deduplizierung auf der Quelle werden wertvolle Systemressourcen auf der Maschine gebunden, wohingegen sich für die Datendeduplizierung nach der Verarbeitung alle notwendigen Daten auf dem Datenträger befinden müssen (d. h. ein höherer anfänglicher Kapazitätsbedarf), bevor der Deduplizierungsprozess beginnt. Die Inline-Datendeduplizierung hingegen benötigt für den Deduplizierungsprozess keine zusätzlichen Datenträgerkapazitäten und CPU-Zyklen auf der Quelle oder auf dem Core. Zuletzt sei noch erwähnt, dass herkömmliche Sicherungsanwendungen jede Woche iterative Komplettsicherungen durchführen, AppAssure hingegen fortlaufende inkrementelle Sicherungen der Maschine auf Blockebene durchführt. Zusammen mit der Datendeduplizierung hilft dieser Ansatz einer fortlaufenden inkrementellen Sicherung dabei, das Gesamtvolumen der auf dem Datenträger gespeicherten Daten um bis zu 80:1 zu reduzieren.

Verschlüsselung

AppAssure umfasst eine integrierte Verschlüsselung, um Sicherungen sowie gespeicherte Daten vor nicht autorisierten Zugriffen und unbefugter Nutzung zu schützen und damit den Datenschutz zu gewährleisten. AppAssure ermöglicht eine starke Verschlüsselung. sodass Sicherungen von geschützten Computern nicht zugänglich sind. Nur der Benutzer mit dem Verschlüsselungsschlüssel kann auf diese Daten zugreifen und sie entschlüsseln. Auf einem System können unbegrenzt viele Verschlüsselungsschlüssel erstellt und gespeichert werden. Der DVM verwendet 256-Bit-AES-Verschlüsselung im CBC-Modus (Cipher Block Chaining) mit 256-Bit-Schlüsseln. Die Verschlüsselung wird inline auf Snapshot-Daten durchgeführt – mit Verbindungsgeschwindigkeit und ohne die Leistung zu beeinträchtigen. Dies liegt daran, dass die DVM-Implementierung Multithread-fähig ist und eine jeweils prozessorspezifische Hardwarebeschleunigung verwendet.

Die Verschlüsselung ist für mehrere Nutzer ausgelegt. Die Deduplizierung wurde speziell auf Datensätze beschränkt, die mit dem gleichen Schlüssel verschlüsselt wurden. Wenn beispielsweise zwei identische Datensätze mit unterschiedlichen Schlüsseln verschlüsselt wurden, werden sie nicht dedupliziert. Dadurch wird sichergestellt, dass im Rahmen der Deduplizierung keine Daten zwischen unterschiedlichen Verschlüsselungsbereichen weitergegeben werden können. Dies ist vorteilhaft für Anbieter verwalteter Dienste, da replizierte Sicherungen für mehrere Nutzer (Kunden) in einem Core gespeichert werden können, ohne dass ein Nutzer die Daten eines anderen Nutzers anzeigen oder darauf zugreifen kann. Jeder Verschlüsselungsschlüssel eines aktiven Nutzers erstellt einen Verschlüsselungsbereich im Repository, in dem nur der Besitzer des Schlüssels die Daten anzeigen, darauf zugreifen oder sie verwenden kann. In einem Szenario mit mehreren Nutzern werden Daten in den Verschlüsselungsbereichen partitioniert und dedupliziert.

In Replikationsszenarien schützt AppAssure die Verbindung zwischen den beiden Cores in einer Replikationstopologie mithilfe von SSL 3.0, um Abhören und Manipulation zu verhindern.

Replikation

Als Replikation wird das Kopieren von Wiederherstellungspunkten von einem AppAssure Core und deren Übertragung auf einen weiteren AppAssure Core an einem anderen Standort bezeichnet, um diese für eine Notfallwiederherstellung verwenden zu können. Dafür ist eine gepaarte Quelle-Ziel-Beziehung zwischen zwei oder mehr Cores erforderlich.

Der Quell-Core kopiert die Wiederherstellungspunkte der ausgewählten geschützten Maschinen und überträgt anschließend die inkrementellen Snapshot-Daten kontinuierlich asynchron zum Ziel-Core in einem Remote-Notfallwiederherstellungsstandort. Sie können ausgehende Replikation an ein unternehmenseigenes Datencenter oder den Remote-Notfallwiederherstellungsstandort (d. h. einen selbstverwalteten Ziel-Core) konfigurieren. Sie können eine ausgehende Replikation auch an einen Drittanbieter, der verwaltete Dienste bereitstellt, (MSP) oder einen Cloud-Anbieter konfigurieren, der externe Sicherungs- und Notfallwiederherstellungsdienste anbietet. Bei der Replikation zu einem Ziel-Core eines Drittanbieters können Sie integrierte Arbeitsabläufe verwenden, mit denen Sie Verbindungen anfordern und automatische Rückmeldungen erhalten können.

Die Replikation wird auf jeder geschützten Maschine einzeln verwaltet. Jede in einem Quell-Core geschützte Maschine kann für die Replikation auf einen Ziel-Core konfiguriert werden.

Abbildung 2. Replikation

Die Replikation ist selbstoptimierend mit einem einzigartigen Read-Match-Write (RMW)-Algorithmus, der eng mit der Deduplizierung verknüpft ist. Bei der RMW-Replikation gleichen der Quell- und Zielreplikationsdienst die Schlüssel vor der Datenübertragung ab. Anschließend werden nur die komprimierten, verschlüsselten, deduplizierten Daten über das WAN übertragen, was eine Reduzierung der erforderlichen Bandbreite um den Faktor 10 ermöglicht.

Die Replikation beginnt mit dem Seeding: Die Erstübertragung von deduplizierten Basisimages und inkrementellen Snapshots von geschützten Agenten, die sich auf hunderte oder tausende Gigabytes an Daten summieren können. Ein Seeding der ersten Replikation auf dem Ziel-Core ist mithilfe externer Medien möglich. Üblicherweise ist das bei umfangreichen Daten oder Standorten mit langsamer Verbindung nützlich. Die Daten im Seeding-Archiv sind komprimiert, verschlüsselt und dedupliziert. Wenn die Gesamtgröße des Archivs den auf dem Wechseldatenträger verfügbaren Speicherplatz überschreitet, kann sich das Archiv, je nach verfügbarem Speicherplatz auf dem Datenträger, über mehrere Geräte erstrecken. Während des Seeding-Vorgangs werden die inkrementellen Wiederherstellungspunkte an den Zielstandort repliziert. Nachdem der Ziel-Core das Seeding-Archiv konsumiert hat, werden die neu replizierten inkrementellen Wiederherstellungspunkte automatisch synchronisiert.

Recovery-as-a-Service (RaaS)

Anbieter von verwalteten Diensten (MSPs) können AppAssure vollständig als Plattform für die Bereitstellung von Wiederherstellung als Service (RaaS, Recovery-as-a-Service) nutzen. RaaS ermöglicht eine vollständige Wiederherstellung in der Cloud (Recovery-in-the-Cloud), indem die physischen und virtuellen Server des Kunden zusammen mit deren Daten in die Cloud des Dienstanbieters als virtuelle Maschinen repliziert werden, um Wiederherstellungstests oder tatsächlichen Wiederherstellungsvorgänge zu unterstützen. Kunden, die eine Wiederherstellung in der Cloud durchführen möchten, können die Replikation der geschützten Maschinen in den lokalen Cores zu einem AppAssure-Dienstanbieter konfigurieren. In einem Notfall können die Anbieter verwalteter Dienste sofort virtuelle Maschinen für den Kunden bereitstellen.

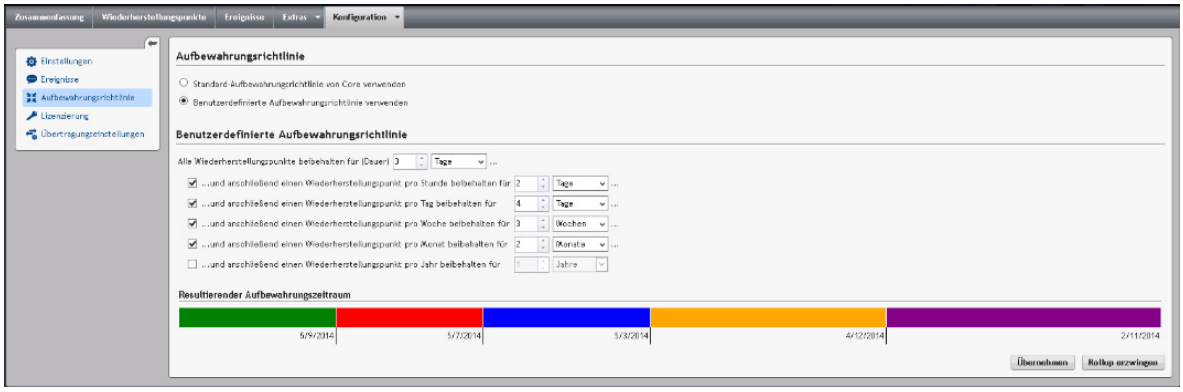
MSPs können eine AppAssure-basierte RaaS-Infrastruktur für mehrere Nutzer bereitstellen, die mehrere und eigenständige Organisationen oder Geschäftseinheiten (die Nutzer) hosten kann, die üblicherweise keine Sicherheitsfunktionen oder Daten auf einem einzelnen Server oder einer Gruppe von Servern gemeinsam nutzen. Die Daten jedes Nutzers sind isoliert und vor anderen Nutzern und dem Dienstanbieter geschützt.

Aufbewahrung und Archivierung

AppAssure ermöglicht flexible Sicherungs- und Aufbewahrungsrichtlinien, die einfach konfiguriert werden können. Die Möglichkeit zur Anpassung der Aufbewahrungsrichtlinien an die Bedürfnisse einer Organisation unterstützt Sie nicht nur bei der Einhaltung von Complianceanforderungen, sondern ermöglicht dies auch ohne Beeinträchtigung der maximal zulässigen Dauer der Wiederherstellung (Recovery Time Objective, RTO).

Aufbewahrungsrichtlinien schreiben den Zeitraum vor, für den Sicherungen auf (schnellen und teuren) Kurzzeitmedien gespeichert werden. Mitunter machen geschäftliche und technische Anforderungen eine längere Aufbewahrung dieser Sicherungen erforderlich. Schnelle Speicher sind jedoch teuer. Deshalb wird durch diese Anforderung (langsame und kostengünstige) Langzeitspeicherung notwendig. Unternehmen verwenden Langzeitspeicher oftmals zur Archivierung von Compliancedaten und anderen Daten. Die Archivierungsfunktion unterstützt die längere Aufbewahrung von Compliancedaten und anderen Daten sowie Seeding von Replikationsdaten auf einem Ziel-Core.

Abbildung 3. Aufbewahrungsrichtlinie



Aufbewahrungsrichtlinien können in AppAssure angepasst werden, um den Zeitraum festzulegen, für den ein Wiederherstellungspunkt aufbewahrt werden soll. Wenn das Alter der Wiederherstellungspunkte das Ende des Aufbewahrungszeitraums erreicht, werden sie als veraltet aus dem Aufbewahrungspool entfernt. Normalerweise wird dieser Prozess ineffizient und schließlich unmöglich, da das Datenvolumen und der Aufbewahrungszeitraum schnell wachsen. AppAssure löst dieses Big Data-Problem, indem die Aufbewahrung großer Datenvolumen mithilfe komplexer Aufbewahrungsrichtlinien verwaltet und Rollup-Vorgänge für die Alterung von Daten mithilfe effizienter Metadatenvorgänge durchführt.

Sicherungen können im Abstand von wenigen Minuten ausgeführt werden und für Tage, Monate und Jahre aufbewahrt werden. Aufbewahrungsrichtlinien verwalten die Alterung und das Löschen alter Sicherungen. Der Alterungsprozess wird durch eine einfache Wasserfallmethode definiert. Die Stufen im Wasserfall werden in Minuten, Stunden und Tagen sowie Wochen, Monaten und Jahren definiert. Die Aufbewahrungsrichtlinie wird durch den nächtlichen Rollup-Prozess erzwungen.

Für eine langfristige Archivierung bietet AppAssure die Möglichkeit, ein Archiv des Quell- oder Ziel-Core auf einem beliebigen Wechseldatenträger zu erstellen. Das Archiv wird intern optimiert. Alle Daten im Archiv werden komprimiert, verschlüsselt und dedupliziert. Wenn die Gesamtgröße des Archivs den auf dem Wechseldatenträger verfügbaren Speicherplatz überschreitet, kann sich das Archiv, je nach verfügbarem Speicherplatz auf dem Datenträger, über mehrere Geräte erstrecken. Für die Wiederherstellung aus einem Archiv ist kein neuer Core erforderlich. Jeder Core kann das Archiv aufnehmen und Daten wiederherstellen, wenn der Administrator über die Passphrase und die Verschlüsselungsschlüssel verfügt.

Virtualisierung und die Cloud

Der AppAssure Core ist Cloud-fähig, d. h., Sie können die Rechenkapazität der Cloud für Wiederherstellung und Archivierung nutzen.

AppAssure kann jede geschützte oder replizierte Maschine in eine virtuelle Maschine (VM) exportieren, z. B. eine lizenzierte Version von VMware oder Hyper-V. Sie können einen einmaligen virtuellen Export durchführen oder durch einen kontinuierlichen virtuellen Export eine Virtual-Standby-VM einrichten. Bei fortlaufenden Exporten wird die virtuelle Maschine inkrementell nach jedem Snapshot aktualisiert. Die inkrementellen Aktualisierungen erfolgen schnell und stellen Standby-Klone bereit, die mit einem Tastenklick eingeschaltet werden können. Die folgenden Exporttypen werden für virtuelle Maschinen unterstützt: VMware Workstation und VMware Server in einem Ordner, direkter Export in einen vSphere oder VMware ESX(i)-Host, Export in Oracle VirtualBox sowie Export in Microsoft Hyper-V Server unter Windows Server 2008 (x64), 2008 R2, 2012 (x64) und 2012 R2 (einschließlich Unterstützung für Hyper-V-VMs der 2. Generation).

Darüber hinaus können Sie Repository-Daten mit Microsoft Azure, Amazon S3, Rackspace Cloud Files oder anderen OpenStack-basierten Cloud-Diensten in der Cloud archivieren.

Benachrichtigungen und Ereignisverwaltung

Neben den HTTP-REST-APIs umfasst AppAssure auch umfangreiche Funktionen für Ereignisprotokollierung und Benachrichtigungen über E-Mails, Syslog oder das Windows-Ereignisprotokoll. Mit E-Mail-Benachrichtigungen können Benutzer oder Gruppen über Zustand oder Status verschiedener Ereignisse benachrichtigt werden. Syslog und Windows-Ereignisprotokoll werden für die zentrale Protokollierung in ein Repository in Umgebungen mit mehreren Betriebssystemen verwendet. In reinen Windows-Umgebungen wird lediglich das Windows-Ereignisprotokoll verwendet.

Lizenzportal

Das Dell Software-Lizenzportal stellt einfach zu verwendende Tools für die Verwaltung der Lizenzberechtigungen bereit. Sie können Lizenzschlüssel herunterladen, aktivieren, anzeigen und verwalten sowie ein Unternehmensprofil zur Nachverfolgung Ihrer Lizenzbestände erstellen. Zusätzlich ermöglicht das Portal es den Dienstanbietern und Wiederverkäufern, ihre Kundenlizenzen nachzuverfolgen und zu verwalten.

Webkonsole

AppAssure verfügt über eine webbasierte zentrale Konsole, die verteilte AppAssure Cores von einem zentralen Standort aus verwaltet. Anbieter von verwalteten Diensten (MSPs) und Unternehmenskunden mit mehreren verteilten Cores können diese Konsole implementieren, um eine einheitliche Ansicht für die zentrale Verwaltung zu erhalten. Mit der AppAssure Central Management Console können Sie die verwalteten Cores in hierarchischen Organisationseinheiten anordnen. Diese Organisationseinheiten können Geschäftseinheiten, Standorte oder Kunden für MSPs mit rollenbasiertem Zugriff darstellen. Mit der zentralen Konsole können Sie auch Berichte für alle verwalteten Cores erstellen.

Dienstverwaltungs-APIs

Zum Lieferumfang von AppAssure gehören mehrere Dienstverwaltungs-APIs, die einen programmgesteuerten Zugriff auf alle Funktionen ermöglicht, die über die AppAssure Central Management Console verfügbar sind. Die Dienstverwaltungs-API ist eine REST-API. Alle API-Vorgänge werden über SSL durchgeführt und gegenseitig mithilfe von X.509 v3-Zertifikaten authentifiziert. Der Verwaltungsdienst ist innerhalb der Umgebung oder direkt über das Internet von jeder Anwendung aus zugänglich, die HTTPS-Anforderungen und -Antworten senden und empfangen kann. Diese Vorgehensweise erleichtert eine einfache Integration in jede beliebige Webanwendung wie RMM-Tools (Relationship Management Methodology) oder Abrechnungssysteme. Darüber hinaus ist in AppAssure ein SDK-Client für die PowerShell-Skripterstellung enthalten.

White-Labeling

Für ausgewählte Unternehmen und OEM-Partner im Platinum-Programm für Dienstanbieter ist ein Rebranding und White-Labeling von AppAssure möglich. Gemäß Platinum-Programm dürfen Partner AppAssure mit ihrem eigenen Namen und Logo sowie Farbdesigns versehen und das Produkt oder den Service mit eigenen Branding und Look-and-feel bereitstellen.

Als AppAssure-Partner können Sie die Software an die jeweiligen Geschäftsanforderungen anpassen. Wenn Sie mehr darüber erfahren möchten, wie Sie AppAssure an Ihre Geschäftsanforderungen anpassen können, wenden Sie sich an den Dell AppAssure-Vertrieb unter sales@software.dell.com, um weitere Informationen zu erhalten.

AppAssure-Assistenten

Bei einem Assistenten handelt es sich um schrittweise Anleitungen, die auf der Benutzeroberfläche in einem Fenster angezeigt werden, um komplexe Aufgaben zu erledigen. Ein Assistent umfasst mindestens zwei Seiten mit Informationen, die der Benutzer angeben muss. (Ein Fenster, das nur eine Seite umfasst, ist ein Dialogfenster.) Assistenten verwenden verschiedenartige allgemein bekannte Grafikkonventionen, um Informationen zu erfassen, z. B. Textfelder, Optionsfelder, Kontrollkästchen und Dropdown-Menüs.

Wenn Sie einen Assistenten starten, wird auf der Benutzeroberfläche ein Fenster geöffnet, in dem Sie durch mehrere Auswahlmöglichkeiten zum Erledigen der Aufgabe geleitet werden. Sie vervollständigen die Informationen auf den einzelnen Seiten des Assistenten abhängig von den jeweiligen Anforderungen. Über die Schaltflächen **Weiter** und **Zurück** können Sie zwischen den Seiten navigieren. Am Ende des Assistenten klicken Sie auf eine Bestätigungsschaltfläche (um die ausgewählten Informationen zu bestätigen und die Aufgabe durchzuführen) oder auf die Schaltfläche **Abbrechen** (um den Assistenten zu beenden, ohne Änderungen vorzunehmen, und dorthin zurückzukehren, wo Sie den Assistenten geöffnet haben).

AppAssure umfasst mehrere Assistenten, die in zwei Kategorien unterteilt werden können.

Zunächst gibt es Assistenten, um die AppAssure-Software und die zugehörigen Komponenten zu installieren, zu aktualisieren oder zu entfernen. Diese werden normalerweise durch Doppelklicken auf ein ausführbares Softwareinstallationsprogramm aufgerufen. Die Installationsprogramme sind durch Herunterladen bestimmter Komponenten vom Dell Software-Lizenzportal zugänglich.

Zweitens sind in der Benutzeroberfläche der AppAssure Core Console Assistenten verfügbar. Diese werden normalerweise durch Klicken auf eine Schaltfläche oder auf einen Link mit aufgerufen, der die Funktion bzw. das Ergebnis des Assistenten angibt. Die Assistenten in dieser Kategorie sind nachstehend aufgelistet.

Tabelle 1.

Name des Assistenten	Aufruf über	Beschreibung
Kurzanleitung	Option „Kurzanleitung“ (Menü „Hilfe“)	Dieser Assistent vereint mehrere Workflows, um häufige Aufgaben für AppAssure zu vereinfachen. Der Benutzer erhält schrittweise Anleitungen, um Maschinen zu schützen, die Replikation für neue Agenten zu konfigurieren, geschützte Daten in virtuelle Maschinen zu exportieren, Wiederherstellungspunktdaten zu verschlüsseln, E-Mail-Benachrichtigungsgruppen zu konfigurieren und eine Aufbewahrungsrichtlinie zu konfigurieren.
Assistent zum Schützen einer Maschine	Schaltfläche „Maschine schützen“ (Symbolleiste)	Dieser Assistent richtet die Schutzfunktion für eine einzelne Maschine ein, die Sie angeben. Sie können einen Namen für die betreffende Maschine eingeben, der in der Core Console angezeigt wird. Wenn die Agent-Software bereits installiert ist, können Sie die Volumes auswählen, die geschützt werden sollen. Andernfalls installiert der Assistent die Software und alle Volumes werden geschützt. Der Assistent legt einen Standardschutzzeitplan fest, bietet aber auch die Möglichkeit, einen benutzerdefinierten Zeitplan festzulegen. Mithilfe der erweiterten Einstellungen können Sie ein Repository auswählen (oder erstellen) und die geschützten Daten verschlüsseln.
Assistent zum Schützen mehrerer Maschinen	Schaltfläche „Massenschutz“ (Registerkarte „Startseite“)	Dieser Assistent richtet die Schutzfunktion auf mehreren Maschinen ein, die Sie angeben. Dabei kann es sich um die Maschinen eines Windows Active Directory-Domänenservers oder eines VMware vCenter Server/ESX(i)-Hosts handeln. Sie können die Maschinen auch manuell als Liste in einem vorgegebenen Format eingeben.
Replikations-assistent	Schaltfläche „Ziel-Core hinzufügen“ (Registerkarte „Replikation“)	Dieser Assistenten richtet die Replikation von einem primären Core (Quell-Core) ein, sodass jederzeit eine Kopie der geschützten Daten auf einem separaten Ziel-Core zur Verfügung steht.

Tabelle 1.

Name des Assistenten	Aufruf über	Beschreibung
Assistent zum Wieder-herstellen einer Maschine	Schaltfläche „Wiederherstellen“ (Symbolleiste)	Dieser Assistent enthält schrittweise Anleitungen, um Daten eines Wiederherstellungspunkts im Core auf eine geschützte Maschine wiederherzustellen oder eine BMR-Wiederherstellung (Bare Metal Restore) einzuleiten.
Exportassistent	Schaltfläche „Export“ (Symbolleiste), Link „Hinzufügen“ (Registerkarte „Virtual Standby“)	Dieser Assistent exportiert Wiederherstellungspunktdaten von einer geschützten Maschine in eine virtuelle Maschine mit einem beliebigen unterstützten VM-Format. Sie können einen einmaligen Export durchführen oder die Virtual Standby-Funktion so einrichten, dass kontinuierlich ein Export erfolgt.

Die Assistenten werden normalerweise verwendet, um Funktionen in AppAssure einzurichten oder zu konfigurieren. Sie können diese Einstellungen später in der Core Console ändern.

2

Arbeiten mit dem AppAssure Core

In diesem Kapitel werden die verschiedenen Aspekte der Verwendung, Konfiguration und Verwaltung des AppAssure Core beschrieben. Folgende Themen werden behandelt:

- Öffnen der AppAssure Core Console
- Navigieren zur AppAssure Core Console.
- Anzeigen und Verwalten geschützter Maschinen
- Informationen zur Kurzanleitung
- Informationen zu benutzerdefinierten Gruppen
- Anleitung zum Konfigurieren des AppAssure Core
- Verwalten von Lizenzen
- Verwalten der AppAssure Core-Einstellungen
- Informationen zu Repositorys
- Anleitung für die Verwaltung eines Repositorys
- Informationen zum Integritätsprüfjob für Repositorys
- Verwalten der Sicherheit
- Verwalten von Cloud-Konten
- Informationen zur Replikation
- Anleitung für die Einrichtung der Replikation
- Replikation auf einen selbstverwalteten Ziel-Core
- Replikation auf den Ziel-Core eines externen Anbieters
- Hinzufügen einer Maschine zu einer bestehenden Replikation
- Konsumieren des Seed-Laufwerks auf einem Ziel-Core
- Verwalten der Replikationseinstellungen
- Aufheben der Replikation
- Wiederherstellen von replizierten Daten
- Anleitung für Failover und Failback
- Verwalten von Ereignissen
- Verwalten der Wiederherstellung
- Informationen zu Systeminformationen
- Herunterladen von Installationsprogrammen
- Informationen zum Agent Installer
- Informationen zum Local Mount Utility
- Verwalten von Aufbewahrungsrichtlinien
- Anleitung für die Archivierung in einer Cloud
- Grundlegende Informationen zu Archiven

- Verwalten von SQL-Anfügbarkeit und Protokollkürzung
- Verwalten von Bereitstellbarkeitsprüfungen und Protokollkürzung für Exchange-Datenbanken
- Statusanzeigen für Wiederherstellungspunkte

Öffnen der AppAssure Core Console

Führen Sie die folgenden Schritte aus, um die AppAssure Core Console zu öffnen.

So öffnen Sie die AppAssure Core Console

- Führen Sie einen der folgenden Schritte aus, um die AppAssure Core Console zu öffnen:
    a Melden Sie sich lokal beim AppAssure Core-Server an, und wählen Sie dann das Symbol für die **Core Console** aus.
    b Sie können auch eine der folgenden URLs im Webbrowser eingeben:
        - https://<CoreServerName>:8006/apprecovery/admin/core oder
        - https://<CoreServerIPAdresse>:8006/apprecovery/admin/core

    HINWEIS: Da die AppAssure Core Console-UI JavaScript verwendet, muss im Webbrowser, mit dem Sie auf die Core Console zugreifen, JavaScript aktiviert sein.

Navigieren zur AppAssure Core Console.

Wenn Sie sich in Release 5.4 bei der AppAssure Core Console anmelden, wird eine aktualisierte Benutzeroberfläche angezeigt. Die Elemente dieser neuen UI sind in der folgenden Tabelle beschrieben.

Tabelle 2.

Element der Benutzeroberfläche	Beschreibung
Kurzanleitung	Bei der Kurzanleitung handelt es sich um eine Folge der vorgeschlagenen Aufgaben zum Konfigurieren und Verwenden von AppAssure. Ab Release 5.4 wird diese Anleitung automatisch geöffnet, wenn Sie sich bei der Core Console anmelden (dies kann deaktiviert werden). Sie können die Kurzanleitung auch im neuen Hilfemenü öffnen. Weitere Informationen zur Kurzanleitung finden Sie unter Informationen zur Kurzanleitung.
Symbolleiste	Die Symbolleiste enthält ein Symbol für jede Registerkarte in der Core Console: „Startseite“, „Replikation“, „Virtual Standby“, „Ereignisse“, „Extras“ und „Konfiguration“.
Menü „Geschützte Maschinen“	Im Menü „Geschützte Maschinen“ können Sie alle Aktionen durchführen, die zuvor nur über die Registerkarte „Maschinen“ zugänglich waren. Weitere Informationen finden Sie unter Anzeigen und Verwalten geschützter Maschinen.

Tabelle 2.

Element der Benutzeroberfläche	Beschreibung
Schaltflächenleiste	Enthält Schaltflächen, die überall in der Core Console zugänglich sind, z. B. „Schützen“, „Wiederherstellen“ und „Export“. Über die Schaltflächen werden Assistenten gestartet, mit denen häufige Aufgaben erledigt werden können, z. B. Schützen einer Maschine, Durchführen einer Wiederherstellung aus einem Wiederherstellungspunkt oder Exportieren von Daten in eine virtuelle Maschine. Wenn Sie auf die Schaltfläche **Schützen** klicken wird standardmäßig der Assistent zum Schützen einer Maschine gestartet. Darüber hinaus umfasst die Schaltfläche „Schützen“ drei Optionen in einem Dropdown-Menü. Über die Option **Maschine schützen** wird ebenfalls der Assistent zum Schützen einer Maschine aufgerufen. Über die Option **Cluster schützen** können Sie eine Verbindung zu einem Server-Cluster herstellen. Über die Option **Massenschutz** wird der Assistent zum Schützen mehrerer Maschinen geöffnet, mit dem Sie zwei oder mehr Maschinen gleichzeitig schützen können.
Anzahl aktiver Aufgaben	Zeigt die Anzahl der Jobs an, die derzeit ausgeführt werden. Dieser dynamische Wert hängt vom Systemzustand ab. Wenn Sie auf das Dropdown-Menü klicken, wird eine Statusübersicht für alle derzeit aktiven Jobs angezeigt. Durch Klicken auf das X für einen Job können Sie den betreffenden Job abbrechen.
Dropdown-Menü „Hilfe“	Dieses Menü enthält folgende Optionen: **Hilfe** (Verknüpfung zur AppAssure-Dokumentationswebsite), **Support** (Verknüpfung zur AppAssure-Supportwebsite, die Zugriff auf Live-Chats, Support-Tickets, Knowledge Base-Artikel usw. ermöglicht), Kurzanleitung (siehe Beschreibung oben) und **Info** (öffnet das Dialogfenster „Info zu AppAssure Core“, das u. a. Versionsinformationen enthält).
Serverdatum und -uhrzeit	Oben rechts in der Core Console werden die aktuelle Uhrzeit und das Datum der Maschine angezeigt, auf der der AppAssure Core-Dienst ausgeführt wird. Diese Zeitangabe wird vom System für Ereignisse verwendet. Bei der Anwendung von Schutzzeitplänen wird beispielsweise die in der Core Console angezeigte Uhrzeit verwendet. Dies gilt auch, wenn die Zeitzone auf dem Datenbankserver oder auf der Clientmaschine, auf der der Browser ausgeführt wird, unterschiedlich ist.
Kontextsensitive Hilfe	Wenn Sie in der AppAssure 5 Core Console auf das Symbol **Hilfe** (blaues Fragezeichen) klicken, wird ein Browserfenster veränderlicher Größe mit zwei Bereichen geöffnet. Der linke Bereich enthält eine Navigationsstruktur, die Themen aus dem *AppAssure 5 Benutzerhandbuch* umfasst. Im rechten Bereich wird der Inhalt des ausgewählten Hilfethemas angezeigt. In der Navigationsstruktur der Hilfe wird immer die Position des ausgewählten Themas in der Hierarchie angezeigt. Mit dieser kontextsensitiven Hilfefunktion können Sie alle Themen des Benutzerhandbuchs durchsuchen. Schließen Sie den Browser, wenn Sie die Hilfethemen nicht mehr benötigen.

Zu den vertrauten Elementen der Benutzeroberfläche zählt der Navigationsbereich im linken Teil, das AppAssure-Logo (über das die AppAssure-Supportwebsite mit direkten Links zur AppAssure-Dokumentation geöffnet werden kann) und mehrere Registerkartensteuerelemente, die die so genannte AppAssure Core Console bilden.

HINWEIS: Benutzer früherer Versionen werden feststellen, dass die Seite „Geschützte Maschinen“, die früher über die Registerkarte „Maschinen“ neben der Registerkarte „Startseite“ in der Core Console aufgerufen werden konnte, nicht mehr vorhanden ist. Alle Funktionen für geschützte Maschinen sind jetzt im Menü „Geschützte Maschinen“ im linken Navigationsbereich zugänglich. Sie können die Seite „Geschützte Maschinen“ ebenfalls über das Menü „Geschützte Maschinen“ öffnen.

Wenn Sie sich bei der Core Console anmelden oder auf das Symbol bzw. die Registerkarte Startseite klicken, wird die Registerkarte „Startseite“ angezeigt und automatisch ausgewählt. Sie können zu jeder anderen Registerkarte wechseln, indem Sie auf den Registerkartennamen oder das entsprechende Symbol klicken.

Zu den anderen Registerkarten, die in der Core Console in Release 5.4 und höher zugänglich sind, zählen „Replikation“, „Virtual Standby“, „Ereignisse“, „Extras“ und „Konfiguration“.

Anzeigen und Verwalten geschützter Maschinen

In der AppAssure-Benutzeroberfläche enthält der linke Navigationsbereich ab Release 5.4 das Menü „Geschützte Maschinen“. In diesem Menü wird standardmäßig eine Liste der Maschinen angezeigt, die durch den jeweiligen Core geschützt werden (sofern welche eingerichtet wurden).

HINWEIS: Im Menü „Geschützte Maschinen“ werden erst dann Maschinen angezeigt, nachdem Maschinen unter den Schutz des Core gestellt wurden.

Das Menü „Geschützte Maschinen“ enthält ein Dropdown-Menü mit den Funktionen, die für die geschützten Maschinen durchgeführt werden können. Klicken Sie auf den Pfeil rechts neben „Geschützte Maschine“, um das Menü anzuzeigen. Dort können Sie die folgenden Aktionen durchführen:

- Erstellung eines inkrementellen Snapshots für alle Maschine erzwingen
- Basisimage für alle Maschinen erzwingen
- Schutz für alle Maschinen vorübergehend deaktivieren (wenn die Schutzfunktion aktiviert ist)
- Schutz für alle Maschinen wieder aktivieren (wenn der Schutz vorübergehend deaktiviert wurde)
- Metadaten für alle geschützten Maschinen aktualisieren

Jede im Menü „Geschützte Maschinen“ aufgelistete Maschine verfügt ebenfalls über ein Dropdown-Menü, das lediglich Funktionen für die jeweilige Maschine steuert. Im Dropdown-Menü einer Maschine können Sie die folgenden Aktionen durchführen:

- Snapshot für die ausgewählte Maschine erzwingen (Sie können Volumes der Maschine auswählen und einen inkrementellen Snapshot oder ein Basisimage auswählen.)
- Schutz für die ausgewählte Maschine vorübergehend deaktivieren (wenn die Schutzfunktion aktiviert ist)
- Schutz wieder aktivieren (wenn der Schutz vorübergehend deaktiviert wurde)
- Metadaten aktualisieren
- Zur Registerkarte „Zusammenfassung“ für die ausgewählte Maschine navigieren
- Zur Registerkarte „Wiederherstellungspunkte“ für die ausgewählte Maschine navigieren
- Zur Registerkarte „Ereignisse“ für die ausgewählte Maschine navigieren
- Zur Registerkarte „Extras“ für die ausgewählte Maschine navigieren (oder eine Funktion auswählen)
- Zur Registerkarte „Konfiguration“ für die ausgewählte Maschine navigieren
- Benutzerdefinierte Beschriftung erstellen, die in der Liste der geschützten Maschinen angezeigt wird

Wenn Sie Cluster im AppAssure Core verwalten, wird der Cluster ebenfalls im linken Navigationsmenü angezeigt. Im Dropdown-Menü eines Clusters können Sie die folgende Aktion durchführen:

- Zur Registerkarte „Geschützte Knoten“ für den ausgewählten Cluster navigieren

Über erweiterbare Dropdown-Untermenüs können Sie schnell zu bestimmten Funktionen für die Maschine navigieren.

- Auf der Registerkarte „Extras“ für eine Maschine können Sie auf alle Funktionen zugreifen, die im erweiterbaren Dropdown-Untermenü „Extras“ verfügbar sind.
- Auf der Registerkarte „Konfiguration“ für eine Maschine können Sie auf alle Funktionen zugreifen, die im erweiterbaren Dropdown-Untermenü „Konfiguration“ verfügbar sind.

Wenn Sie auf den Pfeil links neben dem Menü „Geschützte Maschinen“ klicken, wird die Liste der geschützten Maschinen ausgeblendet, sodass keine Maschinen mehr aufgelistet werden. Wenn Sie erneut auf diesen Pfeil klicken, wird die Liste der Maschinen wieder eingeblendet.

Wenn Sie auf eine Maschine im Menü „Geschützte Maschinen“ klicken, wird die Registerkarte „Zusammenfassung“ für die betreffende Maschine geöffnet. Weitere Informationen zu den Aktionen, die Sie auf der Registerkarte „Zusammenfassung“ erledigen können, finden Sie unter Informationen zur Registerkarte „Zusammenfassung“.

Wenn Sie direkt auf das Menü „Geschützte Maschinen“ klicken wird die Registerkarte „Maschinen“ oder die Seite „Geschützte Maschinen“ im Hauptnavigationsbereich angezeigt, wodurch die Registerkarten „Startseite“, „Replikation“, „Virtual Standby“, „Ereignisse“, „Extras“ und „Konfiguration“ ersetzt werden.

HINWEIS: Auf der Registerkarte „Maschinen“ können Sie zur Ansicht mit mehreren Registerkarten zurückkehren, indem Sie im linken Navigationsbereich auf das Symbol „Startseite“ in der Symbolleiste klicken.

Auf der Registerkarte „Maschinen“ können Sie im Menü „Aktionen“ eine Maschine, zwei oder mehr Maschinen gleichzeitig oder einen Cluster schützen, die Agent-Software auf einer Maschine oder auf mehreren Maschinen bereitstellen (Massenbereitstellung) oder den Assistenten zum Wiederherstellen einer Maschine starten.

Wenn Sie eine geschützte Maschine auswählen, können Sie im Konfigurationsmenü für die jeweilige Maschine einen Snapshot erzwingen, SQL-Protokolldateien kürzen, Daten in eine virtuelle Maschine exportieren, einen Wiederherstellungspunkt bereitstellen, Wiederherstellungspunkte für die betreffende Maschine anzeigen, die ausgewählte Maschine wiederherstellen oder den Schutz der ausgewählten Maschine aufheben.

Informationen zur Registerkarte „Zusammenfassung“

Die Registerkarte „Zusammenfassung“ wird als erste Registerkarte in der AppAssure 5 Core Console angezeigt, wenn Sie eine geschützte Agent-Maschine auswählen. Sie umfasst zumindest einen Zusammenfassungs- und einen Volumes-Bereich.

Informationen zum Zusammenfassungsbereich

Der Zusammenfassungsbereich enthält zusammenfassende Informationen zur geschützten Maschine, z. B. Hostname, Datum und Uhrzeit des letzten Snapshots, Datum und Uhrzeit des nächsten geplanten Snapshots, Informationen zum Verschlüsselungsschlüssel sowie Version der Agent-Software auf der jeweiligen Maschine. Weiterhin ist ein Aktionsmenü vorhanden (siehe Beschreibung unten).

Wenn mindestens ein geschützter Exchange-Server vorhanden ist, gibt es darüber hinaus auch einen Exchange Server-Informationsbereich mit Informationen zu den geschützten Exchange-Servern. Wenn mindestens ein geschützter SQL-Server vorhanden ist, gibt es darüber hinaus auch einen SQL Server-Informationsbereich mit Informationen zu den geschützten SQL-Servern.

Im Dropdown-Menü „Aktionen“ des Zusammenfassungsbereichs können Sie für alle geschützten Maschinen die folgenden Aktionen ausführen:

- **Geschützte Maschine in eine virtuelle Maschine exportieren**. Sie können einen einmaligen Export durchführen oder eine exportierte virtuelle Maschine kontinuierlich aktualisieren. Weitere Informationen finden Sie unter Information zum Exportieren geschützter Daten von Windows-Maschinen in virtuelle Maschinen.
- **Schutz für eine Maschine vorübergehend deaktivieren.** Weitere Informationen finden Sie unter Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion.

- **Metadaten der betreffenden Maschine aktualisieren**. Klicken Sie im Dropdown-Menü „Aktionen“ auf **Metadaten aktualisieren**, um die Metadaten für eine Maschine zu aktualisieren.
- **Maschine aus der Schutzfunktion entfernen**. Dabei können Sie auswählen, ob Wiederherstellungspunkte gelöscht oder beibehalten werden sollen. Weitere Informationen finden Sie unter Entfernen einer Maschine.

Die im Dropdown-Menü „Aktionen“ des Zusammenfassungsbereichs angezeigten Optionen hängen jeweils vom Typ der ausgewählten Maschine ab. Bei SQL-Servern ist beispielsweise eine SQL-Option mit zugehörigen Funktionen im Menü „Aktionen“ vorhanden. Bei Exchange-Servern ist eine Exchange-Option vorhanden.

Im Dropdown-Menü „Aktionen“ des Zusammenfassungsbereichs können Sie für geschützte SQL Server-Maschinen die folgenden Aktionen ausführen:

- **Protokollkürzung erzwingen.** Für eine SQL Server-Maschine können Sie die Kürzung der SQL Server-Protokolle erzwingen. Dabei wird der freie Speicherplatz auf dem SQL-Server ermittelt. Weitere Informationen finden Sie unter Erzwingen einer Protokollkürzung für eine SQL- oder Exchange-Maschine.
- **SQL Server-Anmeldeinformationen festlegen.** Für eine SQL Server-Maschine können Sie die Standardanmeldeinformationen für alle Instanzen oder Instanzanmeldeinformationen für eine einzelne Instanz festlegen. Weitere Informationen finden Sie unter Festlegen der Anmeldeinformationen für SQL-Server.

Im Dropdown-Menü „Aktionen“ des Zusammenfassungsbereichs können Sie für geschützte Exchange Server-Maschinen die folgenden Aktionen ausführen:

- **Protokollkürzung erzwingen.** Für eine Exchange Server-Maschine können Sie die Kürzung der Exchange-Protokolle erzwingen. Dabei wird Speicherplatz auf dem Exchange-Server freigegeben. Weitere Informationen finden Sie unter Erzwingen einer Protokollkürzung für eine SQL- oder Exchange-Maschine.
- **Exchange Server-Anmeldeinformationen festlegen.** Für eine Exchange Server-Maschine können Sie Exchange Server-Einstellungen festlegen oder ändern, z. B. die Kürzung der Exchange Server-Protokolle erzwingen, oder die Anmeldeinformationen für eine Exchange Server-Instanz festlegen. Weitere Informationen finden Sie unter Festlegen der Anmeldeinformationen für Exchange-Server.

Informationen zum Volumes-Bereich

Für jede Agent-Maschine können Sie im Volumes-Bereich der Registerkarte „Zusammenfassung“ die folgenden Aktionen für die aufgelisteten Volumes ausführen:

- **Schutzzeitplan für ein ausgewähltes Volume festlegen oder ändern**. Die Schutzzeitpläne werden normalerweise eingerichtet, wenn eine Maschine erstmals unter Schutz gestellt wird. Weitere Informationen zum Ändern eines Schutzzeitplans finden Sie unter Ändern von Schutzzeitplänen.
- **Erstellung eines Basisimage oder eines Snapshots erzwingen.** Snapshots werden normalerweise gemäß Schutzzeitplan erstellt. Sie können jedoch jederzeit die Erstellung eines Basisimage oder eines inkrementellen Snapshots für ausgewählte Volumes erzwingen. Weitere Informationen finden Sie unter Erzwingen eines Snapshots.

Informationen zur Kurzanleitung

Die Kurzanleitung ist eine neue Funktion in AppAssure, Release 5.4 und höher. Dabei handelt es sich um eine Kurzanleitung der vorgeschlagenen Aufgaben zum Konfigurieren und Verwenden von AppAssure.

Wenn Sie nach der Aktualisierung oder Installation des AppAssure Core zum ersten Mal zur Core Console navigieren, wird automatisch die Kurzanleitung angezeigt. Klicken Sie auf der Begrüßungsseite der Anleitung auf **Kurzanleitung**, um die verschiedenen vorgeschlagenen Konfigurationsaufgaben anzuzeigen. Über die Optionen **Schritt überspringen** und **Zurück** können Sie durch die Anleitung navigieren. Klicken Sie auf **Fertigstellen**, um die Anleitung zu schließen, wenn die letzte vorgeschlagene Aufgabe angezeigt wird.

Sie können die Kurzanleitung jederzeit erneut öffnen. Sie können die Begrüßungsseite in der Kurzanleitung auch ausblenden. Weitere Informationen zu diesen Optionen finden Sie unter Starten der Kurzanleitung.

Die Kurzanleitung wird bei jeder Anmeldung bei der AppAssure Core Console angezeigt, wenn Sie die Registerkarte „Startseite“ aufrufen (sofern Sie sie nicht ausblenden). Weitere Informationen finden Sie unter Ausblenden der Kurzanleitung.

Sie müssen die in der Anleitung vorgeschlagenen Schritte nicht durchführen. Sie können die vorgeschlagenen Aufgaben lediglich anzeigen und mit den Optionen **Schritt überspringen** und **Zurück** zwischen den Aufgaben navigieren. Sie können jederzeit auf **Anleitung beenden** klicken, um die Anleitung auszublenden.

Wenn Sie eine in der Kurzanleitung vorgeschlagene Konfigurationsaufgabe durchführen möchten, folgen Sie den Eingabeaufforderungen in den einzelnen Schritten der Anleitung und dem entsprechenden Assistenten bzw. im relevanten Bereich, der in der Benutzeroberfläche angezeigt wird. Die Vorgehensweise für die Durchführung der einzelnen, in der Anleitung vorgeschlagenen Aufgaben wird in diesem Dokument beschrieben (siehe folgende Tabelle).

HINWEIS: Nicht alle in der Kurzanleitung vorgeschlagenen Konfigurationsaufgaben sind für alle Benutzer erforderlich. Sie müssen wissen, welche Aufgaben Sie für die jeweiligen Anforderungen durchführen müssen.

Die Kurzanleitung deckt die folgenden Konfigurationsaufgaben ab:

Tabelle 3.

Funktion	Kurzbeschreibung	Ergebnis der Ausgabenauswahl, Link zur Vorgehensweise
Schutz	Schützen einer Agent-Maschine, Schützen eines Server-Clusters oder Schützen mehrerer Maschinen mit „Massenschutz“	Klicken Sie auf „Schützen“ oder wählen Sie **Maschine schützen** im Dropdown-Menü aus, um den Assistenten zum Schützen einer Maschine zu öffnen. Informationen zum Durchführen des Assistenten zum Schützen einer Maschine finden Sie unter Schützen einer Maschine. Wählen Sie **Cluster schützen** im Dropdown-Menü aus, um das Dialogfeld „Mit Cluster verbinden“ zu öffnen. Weitere Informationen zum Schützen eines Clusters finden Sie unter Schützen eines Clusters. Wählen Sie im Dropdown-Menü **Massenschutz** aus, um den Assistenten zum Schützen mehrerer Maschinen zu öffnen. Informationen zum Durchführen des Assistenten zum Schützen mehrerer Maschinen finden Sie unter Schützen mehrerer Maschinen.
Replikation	Einrichten der Replikation von einem primären Core (Quell-Core) zu einem sekundären Core (Ziel-Core)	Klicken Sie auf **Replikation**, um die Registerkarte „Replikation“ zu öffnen. Daraufhin werden Sie aufgefordert, mit dem Replikationsassistenten einen Ziel-Core hinzuzufügen. Weitere Informationen zum Einrichten der Replikation auf einem selbstverwalteten Core mit dem Replikationsassistenten finden Sie unter Replikation auf einen selbstverwalteten Ziel-Core. Weitere Informationen zur Replikation finden Sie unter Anleitung für die Einrichtung der Replikation.
Virtueller Export	Durchführen eines einmaligen Exports oder Einrichten eines ständigen Exports von einer geschützten Agent-Maschine in eine virtuelle Maschine	Klicken Sie auf **Export**, um einen Datenexport von einer geschützten Maschine in eine virtuellen Maschine durchzuführen. Sie können einen einmaligen Export durchführen oder die Virtual Standby-Funktion so einrichten, dass kontinuierlich ein Export in eine VM erfolgt. Informationen virtuellen Exporten finden Sie unter Information zum Exportieren geschützter Daten von Windows-Maschinen in virtuelle Maschinen.
Konfiguration	Einrichten weitere Konfigurationseinstellungen für den AppAssure Core	Klicken Sie auf **Konfiguration**, um Einstellungen für Sicherheit (Verschlüsselungsschlüssel einrichten), Benachrichtigungen (Ereignisbenachrichtigungen einrichten) und Aufbewahrungsrichtlinien (Kriterien für Rollup und Alterung von Wiederherstellungspunkten einrichten) anzuzeigen.

Tabelle 3.

Funktion	Kurzbeschreibung	Ergebnis der Ausgabenauswahl, Link zur Vorgehensweise
Konfiguration: Verschlüsselung	Einrichten eines Verschlüsselungsschlüssels, den Sie für einen oder mehrere Agenten verwenden können	Klicken Sie auf **Sicherheit**, um die Seite „Sicherheit“ auf der Registerkarte „Konfiguration“ zu öffnen. Daraufhin werden Sie aufgefordert, einen Verschlüsselungsschlüssel hinzuzufügen oder zu importieren. Danach können Sie ihn auf Agenten anwenden. Die Verschlüsselung wird im Abschnitt Verwalten der Sicherheit behandelt.
Konfiguration: Benachrichtigungen	Einrichten von E-Mail-Benachrichtigungen für Ereignisse, Warnungen und Benachrichtigungen	Klicken Sie auf **Ereignisse**, um Benachrichtigungsgruppen für Ereignisse, Warnungen und Benachrichtigungen anzugeben. Wenn diese per E-Mail gesendet werden sollen, müssen Sie auch SMTP-Servereinstellungen angeben. Weitere Informationen zum Verwalten von Ereignissen finden Sie unter Verwalten von Ereignissen sowie in den Abschnitten Konfigurieren von Benachrichtigungsgruppen und Konfigurieren eines E-Mail-Servers.
Konfiguration: Aufbewahrung	Anzeigen oder Ändern der Standardaufbewahrungsrichtlinie für den Core	Klicken Sie auf **Aufbewahrungsrichtlinie**, um die Seite „Aufbewahrungsrichtlinie“ auf der Registerkarte „Konfiguration“ zu öffnen. Dort können Sie angeben, wie lang ein Wiederherstellungspunkt beibehalten werden soll, bevor ein Rollup erfolgt. Konzeptionelle Informationen zu Aufbewahrungsrichtlinien finden Sie im Abschnitt Aufbewahrung und Archivierung. Informationen zur Vorgehensweise finden Sie unter Verwalten von Aufbewahrungsrichtlinien.
Wiederherstellen	Wiederherstellen von Daten aus einem Wiederherstellungspunkt auf dem Core	Klicken Sie auf **Wiederherstellen**, um den Assistenten zum Wiederherstellen einer Maschine zu öffnen. Informationen zum Wiederherstellen von Daten finden Sie im Abschnitt Wiederherstellen von Volumes aus einem Wiederherstellungspunkt.

Starten der Kurzanleitung

Nach der Aktualisierung oder Installation des AppAssure Core wird automatisch die Kurzanleitung angezeigt. Diese Kurzanleitung wieder immer wieder angezeigt, wenn Sie die Replikation „Startseite“ in der Core Console öffnen (sofern sie nicht ausgeblendet wird).

Gehen Sie folgendermaßen vor, um die Kurzanleitung jederzeit in der Core Console zu öffnen.

So starten Sie die Kurzanleitung

1. Navigieren Sie zur AppAssure Core Console.
2. Klicken Sie im Menü „Hilfe“ auf **Kurzanleitung**.

   Die Kurzanleitung wird angezeigt.

Ausblenden der Kurzanleitung

Nach der Aktualisierung oder Installation des AppAssure Core wird automatisch die Kurzanleitung angezeigt.

Sie wird auch angezeigt, wenn Sie im Dropdown-Menü „Hilfe“ die Option „Kurzanleitung“ auswählen und wenn Sie die Registerkarte „Startseite“ der Core Console öffnen.

Gehen Sie folgendermaßen vor, um die Kurzanleitung auszublenden.

So blenden Sie die Kurzanleitung auf der Begrüßungsseite aus

- Führen Sie in der AppAssure auf der Begrüßungsseite der Kurzanleitung die folgenden Schritte durch:

- Wählen Sie **Dieses Fenster nicht erneut anzeigen** aus, wenn die Begrüßungsseite der Kurzanleitung ausgeblendet werden soll.

  HINWEIS: Dadurch wird die Begrüßungsseite beim Öffnen der Kurzanleitung ausgeblendet, bis der AppAssure Core aktualisiert wird.

- Klicken Sie auf **Schließen**, wenn Sie die Kurzanleitung in dieser Sitzung ausblenden möchten.

  Die Kurzanleitung wird geschlossen. Wenn Sie das nächste Mal die Registerkarte „Startseite“ der Core Console öffnen, wird wieder die Kurzanleitung angezeigt.

  Sie können die Kurzanleitung auch im Menü „Hilfe“ öffnen (siehe Beschreibung in Starten der Kurzanleitung).

So blenden Sie die Kurzanleitung auf einer Seite der Kurzanleitung aus

- Klicken Sie auf einer beliebigen Seite der Kurzanleitung auf **Beenden**.

  Die Kurzanleitung wird geschlossen. Bei Auswahl dieser Option können Sie die Kurzanleitung weiterhin im Menü „Hilfe“ öffnen (siehe Beschreibung in Starten der Kurzanleitung).

Informationen zu benutzerdefinierten Gruppen

Der AppAssure Core enthält im linken Navigationsbereich ein Menü „Geschützte Maschinen“. Dieses enthält alle Maschinen, die unter Schutz durch den AppAssure Core gestellt wurden. Geschützte Cluster (sofern vorhanden) werden ebenfalls im Menü „Geschützte Maschinen“ angezeigt. Darunter werden im Menü „Replizierte Maschinen“ unter dem Namen des replizierten Core die replizierten Maschinen angezeigt (sofern vorhanden). Für alle unter diesen Menüs aufgeführten Maschinen können Sie Gruppenaktionen durchführen, indem Sie auf den Pfeil rechts neben dem Menünamen klicken, um das Dropdown-Menü zu öffnen.

Genauso können Sie eine benutzerdefinierte Gruppe erstellen, die im linken Navigationsbereich angezeigt wird (siehe Beschreibung in Erstellen von benutzerdefinierten Gruppen).

Beim Erstellen einer Gruppen wird immer ein Gruppenmitglied (geschützter Agent, Server-Cluster oder replizierter Agent - abhängig davon, von wo aus die Gruppe erstellt wurde) zu der neuen benutzerdefinierten Gruppe hinzugefügt. Die weiteren Gruppenmitglieder werden im Idealfall anschließend hinzugefügt. Danach können Sie Gruppenaktionen durchführen, die für alle Mitglieder der benutzerdefinierten Gruppe gelten, (siehe Beschreibung in Durchführen von Gruppenaktionen).

Benutzerdefinierte Gruppen können geschützte Agenten, replizierte Agenten und Server-Cluster umfassen. Server-Cluster verhalten sich genauso wie geschützte Agenten, außer dass sich ein Server-Cluster mit den zugehörigen Knoten wie ein einzelnes Objekt verhält. Wenn Sie versuchen, einen Knoten aus einem Server-Cluster zu einer Gruppe hinzuzufügen, wird der gesamte Cluster hinzugefügt.

Eine benutzerdefinierte Gruppe kann ähnliche oder unähnliche Mitglieder enthalten. Bei Gruppen ähnlicher Mitglieder gelten alle Gruppenaktionen für alle Mitglieder der Gruppe. Wenn Sie beispielsweise eine Snapshot-Erstellung für eine benutzerdefinierte Gruppe geschützte Agenten erzwingen, werden alle Agenten gesichert. Bei Gruppen mit unterschiedlichen Mitgliedern (z. B. geschützte Agenten und replizierte Agenten) gilt eine Gruppenaktion wie beispielsweise das Erzwingen einer Replikation nur für replizierte Agenten.

Sie können beliebig viele Gruppen erstellen. Ein einzelner Agent bzw. eine replizierte Maschine kann in mehr als einer Gruppe enthalten sein. Auf diese Weise können Sie Maschinen des Core beliebig gruppieren und Aktionen für die jeweilige Gruppe durchführen.

Alle benutzerdefinierten Gruppen werden im linken Navigationsbereich mit der jeweils festgelegten Bezeichnung angezeigt. Gruppen mit normalen geschützten Agenten werden in der benutzerdefinierten Gruppe angezeigt, dahinter ggf. die replizierten Agenten.

Wenn Sie eine Maschine in eine Gruppe einfügen, wird sie nicht an der ursprünglichen Stelle gelöscht. Wenn beispielsweise drei geschützte Maschinen namens Agent1, Agent2 und Agent3 vorhanden sind, und Sie Agent1 zu CustomGroup1 hinzufügen, wird Agent1 an beiden Stellen angezeigt.

Weitere Informationen finden Sie in den folgenden Abschnitten:

- Erstellen von benutzerdefinierten Gruppen
- Ändern der Namen von benutzerdefinierten Gruppen
- Entfernen von benutzerdefinierten Gruppen
- Durchführen von Gruppenaktionen
- Anzeigen aller Maschinen in einer benutzerdefinierten Gruppe auf einer Seite

Erstellen von benutzerdefinierten Gruppen

Wenn Sie den Cursor über den Namen einer Maschine im Menü „Geschützte Maschinen“ oder „Replizierte Maschinen“ bewegen, wird ein Pfeil angezeigt, über den ein Dropdown-Menü geöffnet wird. In diesem Menü können Sie eine benutzerdefinierte Bezeichnung erstellen.

Gehen Sie folgendermaßen vor, um eine benutzerdefinierte Gruppe zu erstellen.

So erstellen Sie eine benutzerdefinierte Gruppe

1 Navigieren Sie zur AppAssure Core Console.

2 Führen Sie im Menü „Geschützte Maschinen“ oder „Replizierte Maschinen“ die folgenden Aktionen aus:

   a Klicken Sie auf eine Maschine im Menü.

   b Klicken Sie auf das Dropdown-Menü für die betreffende Maschine.

   c Wählen Sie im Menü **Beschriften als** aus, und klicken Sie dann auf **Neue Beschriftung**.

   Daraufhin wird ein neues Menü mit einem leeren Textfeld neben einem Beschriftungssymbol angezeigt. Die ausgewählte Maschine wird unter der benutzerdefinierten Gruppe angezeigt.

3 Geben Sie die gewünschte Bezeichnung für die benutzerdefinierte Gruppe ein.

   Verwenden Sie einen aussagekräftigen Namen, der den Zweck der Gruppe beschreibt. Geben Sie beispielsweise „Buchhaltung“ ein, wenn Agent-Maschinen nach Abteilung gruppiert werden sollen. Sie können eine Gruppe später umbenennen.

   HINWEIS: Die Bezeichnung darf höchstens 50 Zeichen umfassen. Sie können zwischen Wörtern einzelne Leerzeichen eingeben. Sie müssen eine Bezeichnung für die benutzerdefinierte Gruppe eingeben.

4 Klicken Sie auf das grüne Häkchen, wenn Sie die gewünschte Bezeichnung eingegeben haben, um den Namen zu speichern.

   Die Seite wird aktualisiert, sodass die benutzerdefinierte Gruppe im Navigationsbereich angezeigt wird.

5 Um weitere Agenten zu dieser Gruppe hinzuzufügen, können Sie den Namen des Agenten im entsprechenden Menü auswählen, das Dropdown-Menü öffnen, **Beschriften als** auswählen und dann auf den Namen der benutzerdefinierten Gruppe klicken.

   Danach können Sie Gruppenaktionen für diese Gruppe durchführen. Weitere Informationen finden Sie unter Durchführen von Gruppenaktionen.

Ändern der Namen von benutzerdefinierten Gruppen

Wenn Sie den Namen einer benutzerdefinierten Gruppe ändern, wird nur die Bezeichnung geändert. Die Maschinennamen bleiben unverändert.

Gehen Sie folgendermaßen vor, um den Namen einer benutzerdefinierten Gruppe zu ändern.

So ändern Sie den Namen einer benutzerdefinierten Gruppe

1 Navigieren Sie zur AppAssure Core Console.

2 Wählen Sie im Menü „Geschützte Maschinen“ die benutzerdefinierte Gruppe aus, die Sie ändern möchten.

3 Wählen Sie im Dropdown-Menü der betreffenden Gruppe **Bearbeiten** aus.

Der Name der benutzerdefinierten Gruppe kann jetzt bearbeitet werden.

4 Geben Sie eine neue Bezeichnung für die benutzerdefinierte Gruppe ein. Klicken Sie auf das grüne Häkchen, wenn Sie die gewünschte Bezeichnung eingegeben haben, um den Namen zu speichern. Sie können diesen Namen später bearbeiten.

Verwenden Sie einen aussagekräftigen Namen, der den Zweck der Gruppe beschreibt. Geben Sie beispielsweise „Buchhaltung“ ein, wenn Agent-Maschinen nach Abteilung gruppiert werden sollen.

> **HINWEIS:** Die Bezeichnung darf höchstens 50 Zeichen umfassen. Sie können zwischen Wörtern einzelne Leerzeichen eingeben. Sie müssen eine Bezeichnung für die benutzerdefinierte Gruppe eingeben.

5 Um weitere Agenten zu dieser Gruppe hinzuzufügen, können Sie den Namen des Agenten im entsprechenden Menü auswählen, das Dropdown-Menü öffnen, **Beschriften als** auswählen und dann auf den Namen der benutzerdefinierten Gruppe klicken.

Entfernen von benutzerdefinierten Gruppen

Beim Entfernen einer benutzerdefinierten Gruppe wird die betreffende Gruppe aus dem Menü „Geschützte Maschinen“ gelöscht. Die in der Gruppe enthaltenen Maschinen werden nicht gelöscht. Sie befinden sich weiterhin im entsprechenden Standardmenü.

Gehen Sie folgendermaßen vor, um eine benutzerdefinierte Gruppe zu entfernen.

So entfernen Sie eine benutzerdefinierte Gruppe

1 Navigieren Sie zur AppAssure Core Console.

2 Wählen Sie im Menü „Geschützte Maschinen“ die benutzerdefinierte Gruppe aus, die Sie entfernen möchten.

3 Wählen Sie im Dropdown-Menü der betreffenden Gruppe **Beschriftung entfernen** aus.

Daraufhin wird eine Meldung mit der Aufforderung angezeigt, das Entfernen der Gruppe zu bestätigen. Bestätigen Sie die Aktion.

Die Seite wird aktualisiert, sodass die benutzerdefinierte Gruppe nicht mehr im Navigationsbereich angezeigt wird.

Durchführen von Gruppenaktionen

Sie können für jede Gruppe, die in linken Navigationsbereich der AppAssure Core Console angezeigt wird, Gruppenaktionen durchführen. Wenn die Gruppe unterschiedliche Mitglieder enthält (z. B. normale Agent-Maschinen und replizierte Agenten), werden die ausgewählten Aktionen nur für die relevanten Gruppenmitglieder ausgeführt.

Gehen Sie folgendermaßen vor, um Gruppenaktionen für eine benutzerdefinierte Gruppe durchzuführen.

So führen Sie Gruppenaktionen durch

1 Navigieren Sie zur AppAssure Core Console.

2 Wählen Sie im Menü „Geschützte Maschinen“ die benutzerdefinierte Gruppe aus, für die Sie eine Gruppenaktion durchführen möchten.

3 Klicken Sie auf das Dropdown-Menü der betreffenden Gruppe, und wählen Sie dann eine der folgenden Aktionen aus:

- Um einen inkrementellen Snapshot oder ein Basisimage für einen geschützten Agenten zu erzwingen, klicken Sie auf „Snapshot erzwingen“ bzw. auf „Basisimage erzwingen“. Weitere Informationen finden Sie unter Erzwingen eines Snapshots.
- Um den Schutz für einen geschützten Agenten vorübergehend zu deaktivieren, klicken Sie auf **Schutz vorübergehend deaktivieren**. Geben Sie anschließend die Parameter für die Fortsetzung an. Weitere Informationen finden Sie unter Anhalten und Fortsetzen der Replikation.
- Um den Schutz für einen Agenten, für den der Schutz vorübergehend deaktiviert wurde, wieder zu aktivieren, klicken Sie auf „Schutz wieder aktivieren“, und bestätigen Sie, dass der Schutz wieder aktiviert werden soll. Weitere Informationen finden Sie unter Anhalten und Fortsetzen der Replikation.
- Klicken Sie auf **Metadaten aktualisieren**, um die angezeigten Informationen zu aktualisieren.
- Klicken Sie unter „Replikation“ auf **Vorübergehend deaktivieren**, um die Replikation für einen replizierten Agenten auf dem Ziel-Core vorübergehend zu deaktivieren. Weitere Informationen finden Sie unter Anhalten und Fortsetzen der Replikation.
- Klicken Sie unter „Replikation“ auf **Wieder aktivieren**, um die Replikation für einen replizierten Agenten, dessen Replikation auf dem Ziel-Core vorübergehend deaktiviert wurde, wieder zu aktivieren. Weitere Informationen finden Sie unter Anhalten und Fortsetzen der Replikation.
- Klicken Sie auf **Erzwingen**, um die Replikation für eine replizierte Agent-Maschine zu erzwingen. Weitere Informationen finden Sie unter Erzwingen der Replikation.
- Wählen Sie **Bearbeiten** aus, um die Bezeichnung für eine benutzerdefinierte Gruppe zu ändern (nur für benutzerdefinierte Gruppen möglich). Weitere Informationen finden Sie unter Ändern der Namen von benutzerdefinierten Gruppen.
- Wählen Sie **Beschriftung entfernen** aus, um die benutzerdefinierte Gruppe zu entfernen (nur für benutzerdefinierte Gruppen möglich). Weitere Informationen finden Sie unter Entfernen von benutzerdefinierten Gruppen.

Anzeigen aller Maschinen in einer benutzerdefinierten Gruppe auf einer Seite

Wenn Sie auf den Namen einer benutzerdefinierten Gruppe klicken, wird die Registerkarte „Maschinen“ angezeigt, auf der alle Maschinen in der betreffenden Gruppe aufgelistet werden. Dort können Sie einige Funktionen im Menü „Aktionen“ für alle Maschinen durchführen. Sie können Funktionen auch einzeln ausführen, indem Sie Befehle für die jeweilige Maschine auswählen.

Anleitung zum Konfigurieren des AppAssure Core

Damit Sie AppAssure verwenden können, müssen Sie den AppAssure Core konfigurieren.

Sie können die betreffenden Aufgaben einzeln durchführen oder sich in der Kurzanleitung durch die Core-Konfiguration führen lassen. Die Kurzanleitung bietet die Möglichkeit, Assistenten und Konfigurationsschritte zu starten oder lediglich den empfohlenen Ablauf für die Konfigurationsaufgaben anzuzeigen.

Wenn Sie die Konfiguration mithilfe der Kurzanleitung durchführen, wird zuerst eine Maschine mit dem Assistenten zum Schützen einer Maschine geschützt. In diesem Schritt werden Sie aufgefordert, Speicherorte einzurichten. Dies umfasst das Erstellen eines Repositorys und das Festlegen der Repositorygröße. Mithilfe dieser Anleitung können Sie auch Ereignisbenachrichtigungen konfigurieren, Verschlüsselungsschlüssel konfigurieren, die Replikation einrichten, Daten in eine virtuelle Maschine exportieren und die Aufbewahrungsrichtlinie anzeigen oder ändern. Wenn im Core Wiederherstellungspunkte vorhanden sind, können Sie auch Daten wiederherstellen. Informationen zur Kurzanleitung finden Sie unter Informationen zur Kurzanleitung.

Wenn Sie Konfigurationsaufgaben einzeln durchführen, müssen Sie bestimmte Erstkonfigurationsaufgaben durchführen, z. B. Repository zum Speichern von Sicherungs-Snapshots erstellen und konfigurieren, Verschlüsselungsschlüssel zum Schützen der geschützten Daten definieren (optional) und Benachrichtigungen für Aufgaben, Warnungen und Ereignisse einrichten (optional).

Um die Erstkonfiguration des AppAssure Core durchführen zu können, müssen bestimmte Konzepte bekannt sein und bestimmte Anfangsvorgänge durchgeführt werden. Führen Sie zum Konfigurieren des AppAssure Core die folgenden Core-Konfigurationsaufgaben durch:

- **Erstellen eines Repositorys**. Weitere Informationen zu Repositorys finden Sie unter Erstellen eines Repositorys.
- **Konfigurieren von Verschlüsselungsschlüsseln**. Weitere Informationen zum Konfigurieren von Verschlüsselungsschlüsseln finden Sie unter Hinzufügen eines Verschlüsselungsschlüssels.
- **Konfigurieren von Ereignisbenachrichtigungen**. Weitere Informationen zum Konfigurieren von Ereignisbenachrichtigungen finden Sie unter Konfigurieren eines E-Mail-Servers.

Nach der Erstkonfiguration des AppAssure Core können Sie Agent-Maschinen schützen und Daten wiederherstellen. AppAssure umfasst eine Standardaufbewahrungsrichtlinie, die Sie an die jeweiligen Anforderungen anpassen können. Wenn SQL-Datenbanken geschützt werden, können Sie SQL-Anfügbarkeitsprüfungen konfigurieren.

Die weitere Konfiguration des AppAssure Core umfasst die folgenden Vorgänge:

- **Schützen einer einzelnen Agent-Maschine.** Weitere Informationen zum Schützen einer Agent-Maschine mit dem Assistenten zum Schützen einer Maschine finden Sie unter Schützen einer Maschine.
- **Schützen mehrerer Agent-Maschinen.** Weitere Informationen zum Schützen mehrerer Agent-Maschinen in einem Schritt mit dem Assistent zum Schützen mehrerer Maschinen finden Sie unter Schützen mehrerer Maschinen.
- **Wiederherstellen von Daten aus Wiederherstellungspunkten.** Weitere Informationen zum Wiederherstellen von Daten aus Wiederherstellungspunkten mit dem Wiederherstellungsassistenten finden Sie unter Informationen zum Wiederherstellen von Daten aus Wiederherstellungspunkten.
- **Konfigurieren von Aufbewahrungsrichtlinien**. Weitere Informationen zum Konfigurieren von Aufbewahrungsrichtlinien finden Sie unter Verwalten von Aufbewahrungsrichtlinien.
- **Konfigurieren der SQL-Anfügbarkeit**. Weitere Informationen zum Konfigurieren der SQL-Anfügbarkeit finden Sie unter Konfigurieren der SQL-Anfügbarkeitseinstellungen.

Verwalten von Lizenzen

In AppAssure können Sie AppAssure-Lizenzen direkt in der AppAssure Core Console verwalten. In der Konsole können Sie den Lizenzschlüssel ändern und eine Verbindung zum Lizenzserver herstellen. Sie können auf der Seite „Lizenzierung“ in der Konsole auch auf das Dell Software-Lizenzportal zugreifen.

Die Seite „Lizenzierung“ enthält folgende Informationen:

- Lizenztyp
- Lizenzstatus
- Größe des Lizenzpools
- Anzahl der geschützten Maschinen
- Status der letzten Antwort vom Lizenzserver
- Zeitpunkt des letzten Kontakts zum Lizenzserver
- Nächster geplanter Verbindungsversuch mit dem Lizenzserver

Weitere Informationen finden Sie im *Lizenzportal Benutzerhandbuch* auf der Dokumentationswebsite mit AppAssure-Releaseinformationen und -Handbüchern unter https://support.software.dell.com/appassure/release-notes-guides.

Ändern eines Lizenzschlüssels

Führen Sie die nachstehend beschriebenen Schritte aus, um einen Lizenzschlüssel in der AppAssure Core Console zu ändern.

Informationen zum Erwerb eines Lizenzschlüssels finden Sie im *Lizenzportal Benutzerhandbuch* auf der Dokumentationswebsite mit AppAssure-Releaseinformationen und -Handbüchern unter https://support.software.dell.com/appassure/release-notes-guides.

So ändern Sie einen Lizenzschlüssel

1. Navigieren Sie zur AppAssure Core Console und wählen Sie die Registerkarte „Konfiguration“ aus.
2. Klicken Sie auf **Lizenzierung**.

   Die Seite „Lizenzierung“ wird angezeigt.
3. Klicken Sie in den Lizenzdetails auf **Lizenz ändern**.

   Das Dialogfeld „Lizenzschlüssel ändern“ wird angezeigt.
4. Geben Sie im Dialogfeld „Lizenzschlüssel ändern“ den neuen Lizenzschlüssel ein und klicken Sie auf **OK.**

Verbindungsaufbau zum Dell Software-Lizenzportal-Server

Die AppAssure Core Console kontaktiert regelmäßig den Portalserver, damit alle Änderungen, die im Dell Software-Lizenzportal durchgeführt wurden, auf dem neuesten Stand sind. Die Kommunikation mit dem Portalserver erfolgt normalerweise automatisch in bestimmten Zeitabständen. Sie können die Kommunikation jedoch auch bei Bedarf starten.

Führen Sie die nachstehend beschriebenen Schritte aus, um eine Verbindung zum Portalserver herzustellen.

So stellen Sie eine Verbindung zum Portalserver her

1. Navigieren Sie zur AppAssure Core Console und klicken Sie auf die Registerkarte „Konfiguration“.
2. Klicken Sie auf **Lizenzierung**.

   Die Seite „Lizenzierung“ wird angezeigt.
3. Klicken Sie in der Option „Lizenzserver“ auf **Jetzt Kontakt aufnehmen**.

Verwalten der AppAssure Core-Einstellungen

Mit den AppAssure Core-Einstellungen werden verschiedene Einstellungen für Konfiguration und Leistung definiert. Die meisten Einstellungen sind für die optimale Nutzung konfiguriert. Sie können die folgenden Einstellungen aber auch bei Bedarf ändern:

- Allgemein
- Updates
- Nächtliche Jobs
- Übertragungswarteschlange
- Zeitlimiteinstellungen für Client
- Konfiguration des Deduplizierungscache

- Konfiguration der Replay Engine
- Bereitstellungseinstellungen
- Einstellungen für Datenbankverbindung
- SMTP-Servereinstellungen
- Aktivierte Ablaufverfolgungsprotokolle
- Cloud-Konfiguration

Ändern des Core-Anzeigenamens

Führen Sie die nachstehend beschriebenen Schritte aus, um den Core-Anzeigenamen zu ändern.

So ändern Sie den Core-Anzeigenamen

1. Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.

   Das Dialogfeld „Allgemeine Einstellungen“ wird angezeigt.
2. Klicken Sie im Bereich „Allgemein“ auf **Ändern**.

   Das Dialogfeld „Allgemeine Einstellungen“ wird angezeigt.
3. Geben Sie im Textfeld „Anzeigename“ einen neuen Anzeigenamen für den Core ein.

   Dieser Name wird in der AppAssure Core Console angezeigt. Sie können bis zu 64 Zeichen eingeben.
4. Geben Sie im Textfeld „Webserverport“ eine Portnummer für den Webserver ein. Die Standardeinstellung ist 8006.
5. Geben Sie im Textfeld „Dienstport“ eine Portnummer für den Dienst ein. Die Standardeinstellung ist 8006.
6. Klicken Sie auf **OK**.

Konfigurieren von Updateeinstellungen

AppAssure umfasst eine automatische Aktualisierungsfunktion. Bei der Installation des AppAssure Core können Sie auswählen, ob die AppAssure Core-Software automatisch aktualisiert werden soll, wenn Updates verfügbar sind, und wie oft das System Updates suchen soll.

HINWEIS: Informationen zum Installieren der AppAssure Core-Software finden Sie im *Dell AppAssure Bereitstellungshandbuch*.

Sie können die vom System verwendeten Einstellungen für die Suche nach Updates jederzeit anzeigen und ändern.

Führen Sie die folgenden Schritte aus, um Updateeinstellungen zu konfigurieren.

So konfigurieren Sie Updateeinstellungen

1. Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.
2. Klicken Sie im Bereich „Updates“ auf **Ändern**.

   Das Dialogfeld „Aktualisierungseinstellungen“ wird angezeigt.
3. Wählen Sie im Textfeld „Auf neue Aktualisierungen überprüfen“ aus, wie oft Updates gesucht und installiert werden sollen, nachdem die nächtlichen Jobs durchgeführt wurden. Folgende Optionen stehen zur Auswahl:
   - Nie

- Täglich
- Wöchentlich
- Monatlich

4 Geben Sie an, wie Updates verarbeitet werden sollen, wenn sie verfügbar werden. Wählen Sie dazu eine der folgenden Optionen aus:
   - **Automatisch installieren (empfohlen)** oder
   - **Benachrichtigung anzeigen, aber nicht installieren**
5 Klicken Sie auf **OK**.

Konfigurieren nächtlicher Jobs für den Core

Wenn die Option für nächtliche Jobs im AppAssure Core aktiviert ist, wirkt sich dies auf alle Jobs für alle Agenten aus, die vom Core geschützt werden. Wenn Sie diese Option deaktivieren, wirkt sich dies auf alle Agenten aus, die durch den Core geschützt werden.

Nächtliche Jobs können auf Core- oder auf Agent-Ebene angegeben werden. Einige Optionen sind aber nur in der jeweiligen Ebene verfügbar. Auf der Core-Ebene können Sie die nachstehend aufgeführten Joboptionen ausführen:

- Anfügbarkeitsprüfjob
- Die Protokolle werden von den geschützten Maschinen heruntergeladen
- Integrität der Wiederherstellungspunkte prüfen
- Prüfsummenprüfjob
- Rollup
- Protokollkürzungsjob (nur einfaches Wiederherstellungsmodell)
- Repository-Statistik protokollieren
- Alte Ereignisse und Jobs werden gelöscht

Informationen zum Angeben von Joboptionen auf Agentenebene finden Sie unter Anpassen der nächtlichen Jobs für eine geschützte Maschine.

So konfigurieren Sie nächtliche Jobs für den Core

1 Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.
2 Klicken Sie im Bereich „Nächtliche Jobs“ auf **Ändern**.

   Das Dialogfeld „Nächtliche Jobs“ wird angezeigt.
3 Wählen Sie die nächtliche Joboption aus, die Sie für den Core festlegen möchten. Sie können alle auswählen oder die gewünschten Jobs einzeln auswählen.
4 Klicken Sie auf **OK**.

Aktivieren einer nächtlichen Bereitstellungsprüfung

Sie können festlegen, dass der AppAssure Core einen nächtlichen Job für jeden Agenten durchführt, der die Integrität von Wiederherstellungspunkten prüft, indem der letzte Wiederherstellungspunkt für jede Schutzgruppe bereitgestellt wird und die Dateien und Ordner der einzelnen Volumes aufgezählt werden. Die Option „Integrität der Wiederherstellungspunkte prüfen“ überprüft anschließend die Gültigkeit der Wiederherstellungspunkte. Sie können auf Core-Ebene oder für einzelne Agenten angeben, dass nächtliche Bereitstellungsprüfungen durchgeführt werden. Die Option „Integrität der Wiederherstellungspunkte prüfen“ ist standardmäßig nicht aktiviert.

So konfigurieren Sie eine nächtliche Bereitstellungsprüfung für den Core

1. Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.
2. Klicken Sie im Bereich „Nächtliche Jobs“ auf **Ändern**.

   Das Dialogfeld „Nächtliche Jobs“ wird angezeigt.
3. Wählen Sie **Integrität der Wiederherstellungspunkte prüfen** aus.
4. Klicken Sie auf **OK**.

So konfigurieren Sie eine nächtliche Bereitstellungsprüfung für einen Agenten

1. Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.
2. Klicken Sie im Bereich „Nächtliche Jobs“ auf **Ändern**.

   Das Dialogfeld „Nächtliche Jobs“ wird angezeigt.
3. Klicken Sie auf den Abwärtspfeil, um die Ansicht der geschützten Agenten zu erweitern.
4. Wählen Sie die Agenten aus, für die ein nächtlicher Job ausgeführt werden soll, der eine Bereitstellungsprüfung durchführt.
5. Klicken Sie auf **OK**.

Einstellen der Uhrzeit für nächtliche Jobs

Führen Sie die nachstehend beschriebenen Schritte aus, um die Uhrzeit für einen nächtlichen Job einzustellen.

So stellen Sie die Zeit für einen nächtlichen Job ein

1. Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.
2. Klicken Sie im Bereich „Nächtliche Jobs“ auf **Ändern**.

   Das Dialogfeld „Nächtliche Jobs“ wird angezeigt.
3. Geben Sie im Textfeld „Uhrzeit für nächtliche Jobs“ eine neue Uhrzeit für die Ausführung der nächtlichen Jobs ein.
4. Klicken Sie auf **OK**.

Ändern der Einstellungen für die Übertragungswarteschlange

Die Einstellungen für die Übertragungswarteschlange sind Einstellungen auf Core-Ebene, die die maximale Anzahl gleichzeitiger Übertragungen sowie die maximale Anzahl von Wiederholungsversuchen für die Übertragung von Daten festlegen.

Führen Sie die nachstehend beschriebenen Schritte durch, um die Einstellungen für die Übertragungswarteschlange zu ändern.

So ändern Sie die Einstellungen für die Übertragungswarteschlange

1. Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.
2. Klicken Sie im Bereich „Übertragungswarteschlange“ auf **Ändern**.

   Das Dialogfeld „Übertragungswarteschlange“ wird angezeigt.

3 Geben Sie im Textfeld „Maximale Anzahl gleichzeitiger Übertragungen“ einen Wert ein, um die Anzahl gleichzeitiger Übertragungen zu aktualisieren.

   Sie können eine Zahl zwischen 1 und 60 eingeben. Je kleiner die Zahl ist, desto geringer ist die Belastung von Netzwerkressourcen und anderen Systemressourcen. Mit steigender Anzahl verarbeiteter Agenten steigt auch die Belastung des Systems.

4 Geben Sie im Textfeld „Maximale Anzahl der Wiederholungen“ einen Wert ein, um die maximale Anzahl der Wiederholungen zu aktualisieren.

5 Klicken Sie auf **OK**.

Anpassen der Client-Zeitlimiteinstellungen

Führen Sie die nachstehend beschriebenen Schritte aus, um die Einstellungen für das Client-Zeitlimit anzupassen.

So passen Sie die Einstellungen für das Client-Zeitlimit an

1 Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.

2 Klicken Sie im Bereich „Zeitlimiteinstellungen für Client“ auf **Ändern**.

   Das Dialogfeld „Zeitlimiteinstellungen für Client“ wird angezeigt.

3 Geben Sie im Textfeld „Zeitüberschreitung Verbindung“ den Zeitraum in Minuten und Sekunden für das Verbindungszeitlimit ein.

4 Geben Sie im Textfeld „UI-Zeitüberschreitung Verbindung“ den Zeitraum in Minuten und Sekunden für das UI-Verbindungszeitlimit ein.

5 Geben Sie im Textfeld „Zeitüberschreitung Lesen/Schreiben“ den Zeitraum in Minuten und Sekunden für das Zeitlimit von Lese-/Schreibvorgängen ein.

6 Geben Sie im Textfeld „UI-Zeitüberschreitung Lesen/Schreiben“ den Zeitraum in Minuten und Sekunden für das UI-Zeitlimit von Lese-/Schreibvorgängen ein.

7 Klicken Sie auf **OK**.

Grundlegende Informationen zur Größe des Deduplizierungscache sowie zu Speicherorten

Durch die globale Deduplizierung wird der erforderliche Speicherplatz auf den Datenträgern für die gesicherten Daten verringert. Der AppAssure 5-Volume-Manager zur Deduplizierung (DVM) fasst mehrere Speicherorte zu einem einzelnen Repository zusammen. Jedes Repository wird dedupliziert. Dabei werden alle einzigartigen Blocks nur ein Mal physisch auf den Datenträgern gespeichert. In nachfolgenden Sicherungen werden virtuelle Verweise oder Zeiger auf die betreffenden Blöcke verwendet. Um doppelt vorhandene Blöcke zu erkennen, umfasst AppAssure 5 einen Deduplizierungscache, der die Verweise auf die einzigartigen Blöcke enthält.

Dieser Deduplizierungscache ist standardmäßig 1,5 GB groß. Diese Größe ist für viele Repositorys ausreichend. Solange dieser Cache nicht überschritten wird, werden die Daten im ganzen Repository dedupliziert. Sollte der Umfang der redundanten Informationen so umfangreich werden, dass der Deduplizierungscache voll ist, können die Vorteile der Deduplizierung im Repository für neu hinzugefügte Daten nicht vollständig genutzt werden. Der Umfang der im Repository gespeicherten Daten, bevor der Deduplizierungscache voll ist, hängt jeweils von den gesicherten Daten ab und ist für jeden Benutzer unterschiedlich.

Sie können den Deduplizierungscache vergrößern, indem Sie die Konfiguration des Deduplizierungscache im AppAssure 5 Core ändern. Weitere Informationen hierzu finden Sie unter Konfigurieren von Deduplizierungscache-Einstellungen.

Bei eine Vergrößerung des Deduplizierungscache müssen zwei Faktoren berücksichtigt werden: Speicherplatz und RAM-Nutzung.

Speicherplatz. Auf Datenträger werden zwei Exemplare des Cache gespeichert: ein primärer Cache und ein sekundärer Cache (parallele Kopie). Bei einer Standardcachegröße von 1,5 GB ist daher im System ein Speicherplatz von 3 GB erforderlich. Wenn Sie den Cache vergrößern, steigt der Umfang des benötigten Speicherplatzes doppelt proportional zur Cachegröße. Um eine einwandfreie und störungsfreie Leistung sicherzustellen, ändert die Core dynamisch die Priorität dieser Cachespeicher. Beide sind erforderlich. Der einzige Unterschied besteht darin, dass der primäre Cache zuerst gespeichert wird.

RAM-Nutzung. Beim Start des AppAssure Core wird der Deduplizierungscache in den Arbeitsspeicher geladen. Die Speicherbelegung des Systems wird daher von der Cachegröße beeinflusst. Der Gesamtumfang des von Core belegten Arbeitsspeichers hängt von vielen Faktoren ab, z. B. von der Anzahl der aktiven Vorgänge, der Anzahl der Benutzer, der Anzahl der Agenten sowie der Größe des Deduplizierungscache. Jeder Vorgang, der vom Core durchgeführt wird (Übertragung, Replikation, Rollup usw.), belegt zusätzlichen Arbeitsspeicher. Sobald ein Vorgang beendet wurde, sinkt die Speicherbelegung entsprechend. Administratoren müssen jedoch die maximal erforderliche RAM-Nutzung berücksichtigen, damit ein effizienter Betrieb möglich ist.

Bei den Standardeinstellungen für den AppAssure 5 Core werden primärer Cache, sekundärer Cache und Metadaten-Cache im AppRecovery-Verzeichnis von AppAssure 5 gespeichert.

HINWEIS: Abhängig von den jeweiligen Einstellungen ist das Verzeichnis „AppRecovery“ auf dem AppAssure 5 Core nicht sichtbar. Damit das Verzeichnis sichtbar ist, müssen Sie u. U. die Ordneroptionen so ändern, dass versteckte Dateien, Ordner und Laufwerke angezeigt werden.

Sofern der AppAssure 5 Core auf dem Laufwerk C: installiert ist, werden standardmäßig die folgenden Speicherorte verwendet:

Tabelle 4. Standardspeicherorte für den Deduplizierungscache

Einstellung	Standardspeicherort
Speicherort primärer Cache	C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache
Speicherort sekundärer Cache	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
Speicherort Metadaten-Cache	C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

Sie können den Speicherort dieser Cachespeicher ändern. Um die Fehlertoleranz zu erhöhen, können Sie beispielsweise den Speicherort des sekundären Cache auf ein anderes physisches Laufwerk verlagern als der primäre Cache (vorausgesetzt, der AppAssure 5 Core kann auf den Speicherort zugreifen).

Weitere Informationen zum Ändern der Speicherorte für diese Einstellungen finden Sie unter Konfigurieren von Deduplizierungscache-Einstellungen.

Konfigurieren von Deduplizierungscache-Einstellungen

Führen Sie die folgenden Schritte aus, um Deduplizierungscache-Einstellungen zu konfigurieren.

So konfigurieren Sie Deduplizierungscache-Einstellungen

1. Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.
2. Klicken Sie im Bereich „Konfiguration des Deduplizierungscache“ auf **Ändern**.

   Daraufhin wird das Dialogfeld „Konfiguration des Deduplizierungscache“ angezeigt, in dem Sie Speicherort und Größe des Cache angeben können.

   Da der primäre und der sekundäre Cache gleich groß sind, ist zum Speichern dieser beiden Cachespeicher doppelt so viel Speicherplatz erforderlich wie die zugewiesene Deduplizierungscache-Größe. Wenn Sie beispielsweise die Standardgröße von 1,5 GB für den Deduplizierungscache angeben, müssen Sie sicherstellen, dass jeder der beiden Speicherorte über einen Speicherplatz von mindestens 1,5 GB verfügt. Wenn sich beide Speicherorte auf einem Laufwerk befinden (z. B. dem Laufwerk C:), muss mindestens 3,0 GB freier Speicherplatz vorhanden sein.

3 Geben Sie zum Ändern des Speicherorts für den primären Cache im Textfeld „Speicherort primärer Cache“ den Pfad zu einem Speicherort ein, auf den der Core Zugriff hat.

4 Geben Sie zum Ändern des Speicherorts für den sekundären Cache im Textfeld „Speicherort sekundärer Cache“ den Pfad zu einem Speicherort ein, auf den der Core Zugriff hat.

5 Geben Sie zum Ändern des Speicherorts für den Metadaten-Cache im Textfeld „Speicherort Metadaten-Cache“ den Pfad zu einem Speicherort ein, auf den der Core Zugriff hat.

6 Wenn Sie die Größe des Deduplizierungscache ändern möchten, gehen Sie wie folgt vor:

   a Geben Sie im Textfeld „Größe des Deduplizierungscache“ den entsprechenden Wert für den Speicherplatz ein, den Sie für den Deduplizierungscache reservieren möchten.

   Geben Sie beispielsweise 3 in dieses Feld ein, um die Größe des Deduplizierungscache auf 3 GB zu erhöhen.

   b Wählen Sie im Dropdown-Feld für die Größeneinheit „GB“ (Gigabyte) oder „TB“ (Terabyte) aus, um die Maßeinheit für den Wert im Textfeld „Größe des Deduplizierungscache“ anzugeben.

HINWEIS: Die minimale Cachegröße beträgt 1,5 GB. Darüber hinaus darf die Cachegröße nicht größer sein als 50 Prozent des installierten Arbeitsspeichers.

7 Klicken Sie auf **OK**.

HINWEIS: Sie müssen den Core-Dienst neu starten, damit die Änderungen wirksam werden.

Ändern der AppAssureEngine-Einstellungen

Führen Sie die nachstehend beschriebenen Schritte durch, um die AppAssureEngine-Einstellungen zu ändern.

So ändern Sie die AppAssure Engine-Einstellungen

1 Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.

2 Klicken Sie im Bereich „Konfiguration der Replay Engine“ auf **Ändern**.

Das Dialogfeld „Konfiguration der Replay Engine“ wird angezeigt.

3 Geben Sie die Konfigurationsinformationen ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 5.

Textfeld	Beschreibung
IP-Adresse	Wählen Sie eine der folgenden Optionen aus, um die IP-Adresse festzulegen: • Klicken Sie auf **Automatisch bestimmt**, um die bevorzugte IP-Adresse der TCP/IP-Einstellungen zu verwenden. • Oder klicken Sie auf **Verwendung einer spezifischen IP-Adresse**, um eine IP-Adresse manuell einzugeben.
Bevorzugter Port	Geben Sie eine Portnummer ein oder übernehmen Sie die Standardeinstellung. Die Standardportnummer ist *8007*. Der Port wird zur Festlegung des Kommunikationskanals für die AppAssure Engine verwendet.
Verwendeter Port	Stellt den Port dar, der für die Replay Engine-Konfiguration verwendet wird.
Automatische Portzuweisung zulassen	Wählen Sie diese Option aus, um eine automatische TCP-Portzuweisung zuzulassen.
Admin-Gruppe	Geben Sie einen neuen Namen für die Administratorgruppe ein. Der Standardname ist *BUILTIN\Administrators*.

Tabelle 5.

Textfeld	Beschreibung
Minimale Async-E/A-Länge	Geben Sie einen Wert ein oder wählen Sie die Standardeinstellung aus. Dieser Wert beschreibt die minimale asynchrone Eingabe-/Ausgabelänge. Die Standardeinstellung ist *65536*.
Größe des Empfangspuffers	Geben Sie eine Puffergröße für eingehende Daten ein oder übernehmen Sie die Standardeinstellung. Die Standardeinstellung ist *8192*.
Größe des Sendepuffers	Geben Sie eine Puffergröße für ausgehende Daten ein oder übernehmen Sie die Standardeinstellung. Die Standardeinstellung ist *8192*.
Zeitüberschreitung beim Lesen	Geben Sie einen Wert für die Zeitüberschreitung beim Lesen ein oder wählen Sie die Standardeinstellung aus. Die Standardeinstellung ist *00:05:00*.
Zeitüberschreitung beim Schreiben	Geben Sie einen Wert für die Zeitüberschreitung beim Schreiben ein oder wählen Sie die Standardeinstellung aus. Die Standardeinstellung ist *00:05:00*.
Keine Verzögerung	Es wird empfohlen, dieses Kontrollkästchen deaktiviert zu lassen, da andernfalls die Netzwerkleistung beeinträchtigt wird. Falls Sie feststellen, dass diese Einstellung geändert werden muss, wenden Sie sich an den Dell Support, um entsprechende Anweisungen zu erhalten.

4 Klicken Sie auf **OK**.

Ändern von Bereitstellungseinstellungen

Führen Sie die nachstehend beschriebenen Schritte durch, um die Bereitstellungseinstellungen zu ändern.

So ändern Sie Bereitstellungseinstellungen

1 Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.

2 Klicken Sie im Bereich „Bereitstellungseinstellungen“ auf **Ändern**.

Das Dialogfeld „Bereitstellungseinstellungen“ wird angezeigt.

3 Geben Sie in das Textfeld „Agent Installer-Name“ den Namen der ausführbaren Datei für den Agenten ein. Der Standardname ist „Agent-web.exe“.

4 Geben Sie im Textfeld „Core-Adresse“ die Adresse für den Core ein.

5 Geben Sie im Textfeld „Zeitüberschreitung Empfang fehlgeschlagen“ die Wartezeit in Minuten für das Aktivitätszeitlimit ein.

6 Geben Sie im Textfeld „Maximale Anzahl paralleler Installationen“ eine Zahl für die maximale Anzahl von Installationen ein, die parallel durchgeführt werden können.

7 Sie können die folgenden optionalen Einstellungen auswählen:

- **Automatischer Neustart nach Installation**
- **Nach Bereitstellung schützen**

8 Klicken Sie auf **OK**.

Ändern der Datenbankverbindungseinstellungen

Führen Sie die nachstehend beschriebenen Schritte durch, um die Datenbankverbindungseinstellungen zu ändern.

So ändern Sie die Datenbankverbindungseinstellungen

1 Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Einstellungen**.

2 Führen Sie im Bereich „Datenbankverbindungseinstellungen“ einen der folgenden Schritte aus:

- Klicken Sie auf **Standardeinstellungen wiederherstellen**.
- Oder klicken Sie auf **Ändern**.

Das Dialogfeld „Datenbankverbindungseinstellungen“ wird angezeigt.

3 Geben Sie die in der folgenden Tabelle beschriebenen Einstellungen zum Ändern der Datenbankverbindung ein.

Tabelle 6.

Textfeld	Beschreibung
Hostname	Geben Sie einen Hostnamen für die Datenbankverbindung ein.
Port	Geben Sie eine Portnummer für die Datenbankverbindung ein.
Benutzername	(optional) Geben Sie einen Benutzernamen für die Verwaltung der Datenbankverbindungseinstellungen ein. Er wird zur Festlegung von Anmeldeinformationen für den Zugriff auf die Datenbankverbindung verwendet.
Kennwort	(optional) Geben Sie ein Kennwort für die Verwaltung der Datenbankverbindungseinstellungen ein.
Ereignis- und Jobverlauf beibehalten für (Dauer), Tage	Geben Sie die Anzahl an Tagen ein, für die der Ereignis- und Jobverlauf für die Datenbankverbindung aufbewahrt werden soll.
Max. Verbindungspoolgröße	Legt die maximale Anzahl von zwischengespeicherten Datenbankverbindungen fest, um eine dynamische Wiederverwendung zu ermöglichen. Die Standardeinstellung ist 100.
Min. Verbindungspoolgröße	Legt die minimale Anzahl von zwischengespeicherten Datenbankverbindungen fest, um eine dynamische Wiederverwendung zu ermöglichen. Die Standardeinstellung ist 0.

4 Klicken Sie auf **Verbindung testen**, um die Einstellungen zu prüfen.

5 Klicken Sie auf **Speichern**.

Informationen zu Repositorys

In einem Repository werden die Snapshots gespeichert, die von den geschützten Arbeitsstationen und Servern erfasst werden. Das Repository kann sich auf verschiedenen Speichertechnologien wie Storage Area Network (SAN), direkt angeschlossener Speicher oder Network Attached Storage (NAS) befinden.

Wenn Sie ein Repository erstellen, weist der AppAssure Core vorab den Speicherplatz zu, der für die Daten und Metadaten am angegebenen Speicherort erforderlich ist. In einem Core können Sie bis zu 255 unabhängige Repositorys erstellen, die verschiedene Speichertechnologien umfassen können. Darüber hinaus können Sie die Größe eines Repositorys zusätzlich erweitern, indem Sie neue Dateierweiterungen oder -spezifikationen hinzufügen. Ein erweitertes Repository kann bis zu 4096 Erweiterungen enthalten, die verschiedene Speichertechnologien umfassen.

Wichtige Repository-Konzepte und -Überlegungen sind u. a.:

- Das Repository basiert auf dem skalierbaren AppAssure-Objektdateisystem.
- Alle in einem Repository gespeicherten Daten werden global dedupliziert.
- Das skalierbare Objektdateisystem ermöglicht eine skalierbare E/A-Leistung zusammen mit globaler Datendeduplizierung, Verschlüsselung und Aufbewahrungsverwaltung.

HINWEIS: AppAssure-Repositorys müssen auf primären Speichergeräten gespeichert werden. Archivspeichergeräte, z. B. Data Domain-Geräte, werden aufgrund der beschränkten Leistung nicht unterstützt. Ebenso sollten Repositorys nicht auf NAS-Dateiservern gespeichert werden, die an die Cloud gebunden sind, da diese Geräte zu Leistungseinschränkungen neigen, wenn sie als primärer Speicher verwendet werden.

Anleitung für die Verwaltung eines Repositorys

Damit Sie AppAssure nutzen können, müssen Sie mindestens ein Repository auf dem AppAssure Core-Server einrichten. In einem Repository werden die geschützten Daten gespeichert, insbesondere die Snapshots, die von den geschützten Servern in der Umgebung erfasst wurden.

Beim Konfigurieren eines Repositorys können Sie unterschiedliche Aufgaben ausführen, z. B. Festlegen des Speicherorts des Datenspeichers auf dem Core-Server, Festlegen der Anzahl an Speicherorten, die zu den einzelnen Repositorys hinzugefügt werden sollen, Festlegen des Repository-Namens, Festlegen der Anzahl der gleichzeitigen Vorgänge, die Repositorys unterstützen usw.

Wenn Sie ein Repository erstellen, weist der Core vorab den Speicherplatz zu, der für die Daten und Metadaten am angegebenen Speicherort erforderlich ist. Sie können in einem Core bis zu 255 unabhängige Repositorys erstellen. Um die Größe eines Repositorys weiter zu erhöhen, können Sie neue Speicherorte oder Volumes hinzufügen.

Die Verwaltung eines Repositorys umfasst das Erstellen, Konfigurieren und Anzeigen eines Repositorys. Dazu gehören u. a.:

- **Öffnen der Core Console.** Weitere Informationen zum Öffnen der AppAssure Core Console finden Sie unter Öffnen der AppAssure Core Console.
- **Erstellen eines Repositorys.** Weitere Informationen zum Erstellen eines Repositorys finden Sie unter Erstellen eines Repositorys.
- **Anzeigen von Repository-Details.** Weitere Informationen zum Anzeigen von Repository-Details finden Sie unter Anzeigen von Details für ein Repository.
- **Ändern der Repository-Einstellungen.** Weitere Informationen zum Ändern der Repository-Einstellungen finden Sie unter Ändern der Repository-Einstellungen.
- **Hinzufügen neuer Speicherorte.** Weitere Informationen zum Hinzufügen neuer Speicherorte finden Sie unter Hinzufügen eines Speicherorts zu einem vorhandenen Repository.
- **Überprüfen eines Repositorys.** Weitere Informationen zum Überprüfen eines Repositorys finden Sie unter Überprüfen eines Repositorys..
- **Löschen eines Repositorys.** Weitere Informationen zum Löschen eines Repositorys finden Sie unter Löschen eines Repositorys.

Erstellen eines Repositorys

Führen Sie die folgenden Schritte aus, um ein Repository zu erstellen.

So erstellen Sie ein Repository

1 Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:

- Klicken Sie auf der Startseite im Bereich „Repositorys“ auf **Neues Repository hinzufügen**.
- Klicken Sie auf die Registerkarte „Konfiguration“ und klicken Sie auf der Seite „Repositorys“ auf **Neu hinzufügen**.

Das Dialogfeld „Neues Repository hinzufügen“ wird angezeigt.

2 Geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 7.

Textfeld	Beschreibung
Repository-Name	Geben Sie den Anzeigenamen des Repositorys ein. Dieses Textfeld enthält standardmäßig das Wort *Repository* sowie eine Indexnummer, die der Nummer des neuen Repositorys entspricht. Sie können den Namen bei Bedarf ändern. Sie können bis zu 40 Zeichen eingeben.
Gleichzeitige Vorgänge	Legen Sie die Anzahl gleichzeitiger Anforderungen fest, die das Repository unterstützen soll. Der Standardwert ist *64*.
Anmerkungen	Geben Sie eine beschreibende Anmerkung zu diesem Repository ein. Sie können bis zu 254 Zeichen eingeben.

3 Klicken Sie auf **Speicherort hinzufügen**, um den jeweiligen Speicherort oder das Volume für das Repository festzulegen.

WARNUNG: Wenn das AppAssure-Repository, das Sie in diesem Schritt erstellen, später entfernt wird, werden alle Dateien am Speicherort des Repositorys gelöscht. Wenn Sie keinen dedizierten Ordner zum Speichern der Repositorydateien festlegen, werden die betreffenden Dateien im Stammverzeichnis gespeichert. Wird das Repository gelöscht, wird auch der gesamte Inhalt des Stammverzeichnisses gelöscht, sodass es zu einem katastrophalen Datenverlust kommt.

HINWEIS: AppAssure-Repositorys müssen auf primären Speichergeräten gespeichert werden. Archivspeichergeräte, z. B. Data Domain-Geräte, werden aufgrund der beschränkten Leistung nicht unterstützt. Ebenso sollten Repositorys nicht auf NAS-Dateiservern gespeichert werden, die an die Cloud gebunden sind, da diese Geräte zu Leistungseinschränkungen neigen, wenn sie als primärer Speicher verwendet werden.

Das Dialogfeld „Speicherort hinzufügen“ wird angezeigt.

4 Geben Sie im Bereich „Speicherort“ an, wie die Datei für den Speicherort hinzugefügt werden soll. Sie können die Datei auf einem lokalen Datenträger oder auf einer CIFS-Freigabe hinzufügen.

- Wählen Sie **Datei auf lokalem Datenträger hinzufügen** aus, um eine lokale Maschine anzugeben, und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 8.

Textfeld	Beschreibung
Datenpfad	Geben Sie den Speicherort für die geschützten Daten ein. Geben Sie beispielsweise `X:\Repository\Data` ein. Für den Pfad gelten ebenfalls die oben genannten Einschränkungen: Verwenden Sie nur alphanumerische Zeichen, Bindestrich oder Punkt und keine Leerzeichen oder Sonderzeichen.
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

- Wählen Sie **Datei auf CIFS-Freigabe hinzufügen** aus, um eine Netzwerkfreigabe als Speicherort anzugeben, und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 9.

Textfeld	Beschreibung
UNC-Pfad	Geben Sie den Pfad für den Speicherort der Netzwerkfreigabe ein. Definieren Sie einen dedizierten Ordnernamen (z. B. `Repository`), wenn sich der Speicherort im Stammverzeichnis befindet. Der Pfad muss mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für den Zugriff auf den Speicherort der Netzwerkfreigabe an.
Kennwort	Geben Sie ein Kennwort für den Zugriff auf den Speicherort der Netzwerkfreigabe an.

5 Klicken Sie im Bereich „Speicherkonfiguration“ auf **Weitere Details**, und geben Sie dann die Details für den Speicherort ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 10.

Textfeld	Beschreibung
Größe	Legen Sie die Größe oder Kapazität für den Speicherort fest. Der Standardwert ist 250 MB. Sie können zwischen folgenden Optionen wählen: • MB • GB • TB **HINWEIS:** Die angegebene Größe darf die Größe des Volumes nicht überschreiten. Wenn es sich beim Speicherort um ein NTFS-Volume (New Technology File System) unter Windows XP oder Windows 7 handelt, ist die Dateigröße auf 16 TB beschränkt. Wenn es sich beim Speicherort um ein NTFS-Volume (New Technology File System) unter Windows 8, 8.1 oder Windows Server 2012, 2012 R2 handelt, ist die Dateigröße auf 256 TB beschränkt. **HINWEIS:** Damit AppAssure das Betriebssystem überprüfen kann, muss die Windows-Verwaltungsinstrumentation (WMI) auf dem beabsichtigten Speicherort installiert sein.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung *Ein* steuert Windows das Caching. **HINWEIS:** Wenn die Schreib-Caching-Richtlinie auf *Ein* festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie eine Version von Windows Server vor Server 2012, ist die empfohlene Einstellung *Aus*. Bei Auswahl von *Aus* steuert AppAssure das Caching. Bei Auswahl von *Sync* steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist *512*.
Durchschnittliche Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist *8192*.

6 Klicken Sie auf **Save**.

Der neu hinzugefügte Speicherort wird im Bildschirm „Repositorys“ angezeigt.

7 Wiederholen Sie ggf. Schritt 3 bis Schritt 6, um weitere Speicherorte für das Repository hinzuzufügen.

8 Klicken Sie auf **Erstellen**, um das Repository zu erstellen.

Das Repository wird in der Registerkarte „Konfiguration“ angezeigt.

Anzeigen von Details für ein Repository

Führen Sie den folgenden Schritt aus, um Details für ein Repository anzuzeigen.

So zeigen Sie Details für ein Repository an

- Klicken Sie in der AppAssure Core Console auf die Registerkarte „Konfiguration“.

  Die Seite „Repositorys“ wird angezeigt.

- Klicken Sie auf das Symbol der rechten spitzen Klammer > neben der Spalte „Status“ des Repositorys, dessen Details Sie anzeigen möchten.
- Über das Symbol „Einstellungen“ neben der Spalte „Komprimierungsverhältnis“ können Sie die folgenden Aktionen für ein Repository durchführen:
    - Einstellungen ändern
    - Speicherort hinzufügen
    - Repository überprüfen
    - Repository löschen
- Die angezeigten Details für ein Repository umfassen auch Speicherorte und Statistiken. Die Details für Speicherorte umfassen:
    - Metadatenpfad
    - Datenpfad
    - Größe

  Die folgenden statistischen Informationen stehen zur Verfügung:
    - Deduplizierung
    - Datensatz E/A
    - Speichermodul

  Für die Deduplizierung werden als verfügbare Details die Anzahl der Blockdeduplizierungstreffer, die Anzahl der Blockdeduplizierungsfehler und die Blockkomprimierungsrate gemeldet.

  Für Datensatz E/A umfassen die Details Geschwindigkeit (MB/s), Lesegeschwindigkeit (MB/s) und Schreibgeschwindigkeit (MB/s).

  Die Speichermoduldetails umfassen Geschwindigkeit (MB/s), Lesegeschwindigkeit (MB/s) und Schreibgeschwindigkeit (MB/s).

Ändern der Repository-Einstellungen

Nachdem Sie ein Repository hinzugefügt haben, können Sie die Repository-Einstellungen wie die Beschreibung oder die maximale Anzahl gleichzeitiger Vorgänge ändern. Außerdem können Sie einen neuen Speicherort für das Repository hinzufügen. Weitere Informationen zum Hinzufügen neuer Speicherorte finden Sie unter Hinzufügen eines Speicherorts zu einem vorhandenen Repository.

So ändern Sie die Repository-Einstellungen

1 Klicken Sie in der AppAssure Core Console auf die Registerkarte „Konfiguration“.

  Die Seite „Repositorys“ wird angezeigt.

2 Klicken Sie auf das Symbol „Einstellungen“ neben der Spalte „Komprimierungsverhältnis“ unter der Schaltfläche „Aktionen“ und dann auf **Einstellungen**.

  Das Dialogfeld „Repository-Einstellungen“ wird angezeigt.

3 Bearbeiten Sie die in der folgenden Tabelle beschriebenen Repository-Informationen.

Tabelle 11.

Textfeld	Beschreibung
Repository-Name	Stellt den Anzeigenamen des Repositorys dar. Dieses Textfeld enthält standardmäßig das Wort „Repository“ sowie eine Indexnummer, die der Nummer des Repositorys entspricht. HINWEIS: Sie können den Repository-Namen nicht bearbeiten.
Beschreibung	Geben Sie eine beschreibende Anmerkung zum Repository ein (optional).
Maximale Anzahl gleichzeitiger Vorgänge	Legen Sie die Anzahl gleichzeitiger Anforderungen fest, die das Repository unterstützen soll.
Deduplizierung aktivieren	Deaktivieren Sie dieses Kontrollkästchen, um die Deduplizierung zu deaktivieren. Aktivieren Sie dieses Kontrollkästchen, um die Deduplizierung zu aktivieren. HINWEIS: Eine Änderung dieser Einstellung gilt nur für Sicherungen, die nach der Änderung erstellt werden. Vorhandene Daten bzw. Daten, die von einem anderen Core repliziert oder aus einem Archiv importiert wurden, behalten die Deduplizierungseinstellung, die bei der Erfassung der Daten von einem Agenten wirksam war.
Komprimierung aktivieren	Deaktivieren Sie dieses Kontrollkästchen, um die Komprimierung zu deaktivieren. Aktivieren Sie dieses Kontrollkästchen, um die Komprimierung zu aktivieren. HINWEIS: Eine Änderung dieser Einstellung gilt nur für Sicherungen, die nach der Änderung erstellt werden. Vorhandene Daten bzw. Daten, die von einem anderen Core repliziert oder aus einem Archiv importiert wurden, behalten die Komprimierungseinstellung, die bei der Erfassung der Daten von einem Agenten wirksam war.

4 Klicken Sie auf **Speichern**.

Hinzufügen eines Speicherorts zu einem vorhandenen Repository

Durch das Hinzufügen eines Speicherortes können Sie definieren, wo das Repository oder das Volume gespeichert werden soll. Führen Sie die folgenden Schritte aus, um den Speicherort für das Repository oder Volume anzugeben.

So fügen Sie einen Speicherort zu einem vorhandenen Repository hinzu

1 Klicken Sie auf das Symbol „Einstellungen“ neben der Spalte „Komprimierungsverhältnis“ unter der Schaltfläche „Aktionen“ und dann auf **Speicherort hinzufügen**.

Das Dialogfeld „Speicherort hinzufügen“ wird angezeigt.

2 Geben Sie an, wie die Datei für den Speicherort hinzugefügt werden soll. Sie können die Datei auf einem lokalen Datenträger oder auf einer CIFS-Freigabe hinzufügen.

- Wählen Sie **Datei auf lokalem Datenträger hinzufügen** aus, um eine lokale Maschine anzugeben, und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 12.

Textfeld	Beschreibung
Metadatenpfad	Geben Sie den Speicherort für die geschützten Metadaten ein. Geben Sie beispielsweise `X:\Repository\Metadata` ein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Datenpfad	Geben Sie den Speicherort für die geschützten Daten ein. Geben Sie beispielsweise `X:\Repository\Data` ein. Für den Pfad gelten ebenfalls die oben genannten Einschränkungen: Verwenden Sie nur alphanumerische Zeichen, Bindestrich oder Punkt und keine Leerzeichen oder Sonderzeichen.

- Wählen Sie **Datei auf CIFS-Freigabe hinzufügen** aus, um eine Netzwerkfreigabe als Speicherort anzugeben, und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 13.

Textfeld	Beschreibung
UNC-Pfad	Geben Sie den Pfad für den Speicherort der Netzwerkfreigabe ein. Definieren Sie einen dedizierten Ordnernamen (z. B. `Repository`), wenn sich der Speicherort im Stammverzeichnis befindet. Der Pfad muss mit \\ beginnen. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.
Benutzername	Geben Sie einen Benutzernamen für den Zugriff auf den Speicherort der Netzwerkfreigabe an.
Kennwort	Geben Sie ein Kennwort für den Zugriff auf den Speicherort der Netzwerkfreigabe an.

3 Klicken Sie im Bereich „Speicherkonfiguration“ auf **Weitere Details**, und geben Sie dann die Details für den Speicherort ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 14.

Textfeld	Beschreibung
Größe	Legen Sie die Größe oder Kapazität für den Speicherort fest. Die Standardgröße beträgt 250 MB. Sie können zwischen folgenden Optionen wählen: • MB • GB • TB **HINWEIS:** Die angegebene Größe darf die Größe des Volumes nicht überschreiten. Wenn es sich beim Speicherort um ein NTFS-Volume (New Technology File System) unter Windows XP oder Windows 7 handelt, ist die Dateigröße auf 16 TB beschränkt. Wenn es sich beim Speicherort um ein NTFS-Volume (New Technology File System) unter Windows 8, 8.1 oder Windows Server 2012, 2012 R2 handelt, ist die Dateigröße auf 256 TB beschränkt. **HINWEIS:** Damit AppAssure das Betriebssystem überprüfen kann, muss die Windows-Verwaltungsinstrumentation (WMI) auf dem beabsichtigten Speicherort installiert sein.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung *Ein* steuert Windows das Caching. **HINWEIS:** Wenn die Schreib-Caching-Richtlinie auf *Ein* festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie eine Version von Windows Server vor Server 2012, ist die empfohlene Einstellung *Aus*. Bei Auswahl von *Aus* steuert AppAssure das Caching. Bei Auswahl von *Sync* steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist *512*.
Durchschnittliche Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist *8192*.

4 Klicken Sie auf **Speichern**.

Der neu hinzugefügte Speicherort wird im Bildschirm „Repositorys“ angezeigt.

5 Wiederholen Sie ggf. Schritt 3 bis Schritt 6, um weitere Speicherorte für das Repository hinzuzufügen.

6 Klicken Sie auf **OK**.

Überprüfen eines Repositorys.

Mit AppAssure können Sie im Falle von Fehlern eine Diagnoseprüfung eines Repository-Volumes durchführen. Core-Fehler können durch fehlerhaftes Herunterfahren, Hardwarefehler usw. verursacht werden.

HINWEIS: Die folgenden Schritte sollte nur zu Diagnosezwecken durchgeführt werden, z. B. bei einem Hardwarefehler, bei einem fehlerhaften Herunterfahren des Core, Fehler beim Importieren eines Repositorys usw.

So überprüfen Sie ein Repository

1. Klicken Sie auf das Symbol „Einstellungen“ neben der Spalte „Komprimierungsverhältnis“ unter der Schaltfläche „Aktionen“ und dann auf **Überprüfen**.

   Das Dialogfeld „Repository überprüfen“ wird angezeigt.

2. Klicken Sie im Dialogfeld „Repository überprüfen“ auf **Überprüfen**.

   HINWEIS: Bei der Durchführung einer Überprüfung werden alle aktiven Aufgaben für das jeweilige Repository abgebrochen. Vor Beginn der Überprüfung wird eine Meldung mit der Frage angezeigt, ob die Überprüfung wirklich durchgeführt werden soll. Sie sollten an dieser Stelle den Cache für Wiederherstellungspunkte neu erstellen, damit dieser auf dem aktuellen Stand ist, da das Repository aus einem Archiv wiederhergestellt werden muss, wenn die Überprüfung fehlschlägt.

Löschen eines Repositorys

Führen Sie die folgenden Schritte aus, um ein Repository zu löschen.

So löschen Sie ein Repository

1. Klicken Sie auf das Symbol „Einstellungen“ neben der Spalte „Komprimierungsverhältnis“ unter der Schaltfläche „Aktionen“ und dann auf **Löschen**.
2. Klicken Sie im Dialogfeld „Repository löschen“ auf **Löschen**.

   In einer Warnmeldung werden Sie aufgefordert, den Löschvorgang zu bestätigen.
3. Klicken Sie auf **Ja**, um das Löschen des Repositorys zu bestätigen.

VORSICHT: Wenn ein Repository gelöscht wird, werden die Daten im Repository verworfen und können nicht wiederhergestellt werden.

Informationen zum Integritätsprüfjob für Repositorys

In früheren Releases wurden Wiederherstellungspunkte im Rahmen der Replikation regelmäßig vom Quell-Core zum Ziel-Core kopiert. Ein Rollup veralteter Wiederherstellungspunkte wurde aber nur auf dem Quell-Core durchgeführt. Zusammengehörige ältere Wiederherstellungspunkte wurden bei der Ausführung des nächtlichen Jobs synchronisiert.

Ab Version 5.4.1 umfasst AppAssure 5 die Möglichkeit, unterschiedliche Aufbewahrungsrichtlinien für Quell-Core und Ziel-Core festzulegen, sofern Quell-Core und Ziel-Core dieselbe Version (5.4.1 oder höher) aufweisen. AppAssure-Administratoren können so Rollups auf einem Ziel-Core mit einer anderen (schnelleren) Rate als auf dem Quell-Core konfigurieren. Ebenso können Sie jetzt eine benutzerdefinierte Aufbewahrungsrichtlinie für replizierte Agenten festlegen, wobei Rollups von Wiederherstellungspunkten im Ziel-Core in kürzeren Abständen und weniger granulär als im Quell-Core durchgeführt werden, um Speicherlpatz zu sparen. Weitere Informationen finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für einen Agenten.

Von einigen Kunden wurden vor AppAssure 5 Release 5.3.6 Inkonsistenzen in Wiederherstellungspunkten festgestellt, die auf einen Ziel-Core repliziert wurden. Um dieses Problem zu beheben, umfasst AppAssure 5

Release 5.4.1 und höher einen neuen Integritätsprüfjob, der für jedes Repository durchgeführt werden muss, damit unterschiedliche Aufbewahrungsrichtlinien auf dem Quell-Core und einem Ziel-Core bzw. benutzerdefinierte Aufbewahrungsrichtlinien für einen replizierten Agenten konfiguriert werden können.

Bei der Ausführung des Integritätsprüfjobs überprüft das System die Integrität aller Daten, die im angegebenen Repository gespeichert sind, damit Daten aus allen Snapshot- oder Basisimages wiederhergestellt werden können. Falls bei der Integritätsprüfung ein Problem mit den Daten im Repository festgestellt wird, wird der Job sofort beendet. In den Ereignisdetails für den betreffenden Job auf dem Core werden Sie aufgefordert, Kontakt zum Dell AppAssure Support aufzunehmen, damit Sie zusammen mit einem Dell Mitarbeiter zu einem vereinbarten Zeitpunkt weitere Schritte durchführen können, um Dateninkonsistenzen zu ermitteln und zu beheben.

△ **VORSICHT: Die Ausführung dieses Jobs kann abhängig vom Datenvolumen im Repository und vom zugrunde liegenden Speichersystem erhebliche Zeit in Anspruch nehmen. Während der Jobausführung können keine anderen Transaktionen im jeweiligen Repository durchgeführt werden, z. B. Übertragungen (Snapshot- und Basisimage-Sicherungen sowie Replikationen), nächtliche Jobs usw.**

Sie können andere Vorgänge in anderen Repositorys durchführen, während der Integritätsprüfjob ausgeführt wird.

ⓘ **HINWEIS:** Im Rahmen dieses Jobs wird die Integrität *aller Inhalte* in einem Repository überprüft. Informationen zum Repositoryprüfjob, mit dem Sie feststellen können, ob ein Repository bereitgestellt und genutzt werden kann, finden Sie unter Überprüfen eines Repositorys..

Dabei handelt es sich um einen Ad-hoc-Job, der für die einzelnen Repositorys ausgeführt werden kann. Dell empfiehlt bei einem Upgrade von Release 5.3.x, den Integritätsprüfjob einmalig für jedes Repository auf einem replizierten Ziel-Core durchzuführen.

Sie brauchen diesen Job *nicht* durchzuführen, wenn eine der folgenden Bedingungen erfüllt ist:

- Es handelt sich um ein neues Repository auf einem Ziel-Core, das in Release 5.4.1 oder höher erstellt wurde.
- Es handelt sich um einen Quell-Core.
- Für das betreffende Repository wurde der Integritätsprüfjob bereits durchgeführt.
- Die Replikationsfunktion wurde nicht verwendet.

Anweisungen zum Durchführen dieser Prüfung finden Sie unter Ausführen des Integritätsprüfjobs für ein Repository.

Ausführen des Integritätsprüfjobs für ein Repository

Führen Sie die folgenden Schritte aus, um die Integrität des ganzen Repositorys zu überprüfen. Sie sollten diese Schritte für replizierte Ziel-Cores ausführen, wenn Sie ein Upgrade von AppAssure 5.3.x auf Release 5.4 durchführen. Während der Ausführung der Integritätsprüfung, die recht zeitaufwändig sein kann, können keinen anderen Aktionen im Repository durchgeführt werden.

Führen Sie diese Schritte einmal für jedes Repository durch, wenn mehrere Repositorys für einen Ziel-Core vorhanden sind.

ⓘ **HINWEIS:** Wenn ein anderes Repository im Ziel-Core vorhanden ist, für das der Integritätsprüfjob bereits durchgeführt wurde, oder wenn Sie ein neues zusätzliches Repository für diesen Ziel-Core erstellen, können Sie im jeweiligen zweiten Repository Vorgänge durchführen, während der Integritätsprüfjob für das primäre Repository ausgeführt wird.

So führen Sie den Integritätsprüfjob für Repositorys aus

1 Navigieren Sie zur AppAssure 5 Core Console, klicken Sie auf die Registerkarte **Konfiguration** und dann auf **Repositorys**.

Auf der Seite „Repositorys“ wird eine Liste der zu diesem Core gehörenden Repositorys angezeigt.

2 Wählen Sie im Dropdown-Menü für das zu überprüfende Repository **Integritätsprüfung** aus.

Daraufhin wird eine Bestätigungsmeldung angezeigt.

△ **VORSICHT: Bevor Sie bestätigen, dass der Job durchgeführt werden soll, sollten Sie unbedingt die dafür erforderliche Zeit beachten. Während der Jobausführung können keine anderen Transaktionen im jeweiligen Repository durchgeführt werden, z. B. Übertragungen (Snapshot- und Basisimage-Sicherungen sowie Replikationen), nächtliche Jobs usw.**

3 Klicken Sie im Dialogfenster „Integrität des Repositorys überprüfen“ auf **Ja**, um die Integritätsprüfung durchzuführen.

Das Dialogfenster „Integrität des Repositorys überprüfen“ wird geschlossen. Alle Jobs in der Warteschlange und alle laufenden Jobs werden abgebrochen, und der Integritätsprüfjob beginnt.

4 Klicken Sie auf die Registerkarte **Ereignisse**, um den Fortschritt des Integritätsprüfjobs für ein Repository zu überwachen und festzustellen, ob ggf. weitere Schritte erforderlich sind.

5 Klicken Sie auf der Seite „Ereignisse“ auf **Details anzeigen** für den Job, um weitere Informationen zum Jobstatus anzuzeigen.

- Falls in einer untergeordneten Aufgabe dieses Jobs ein Fehler angezeigt wird, notieren Sie sich den Fehler und übergeben Sie die Informationen an einen Mitarbeiter des technischen Supports von Dell.
- Wenn alle untergeordneten Aufgaben des Integritätsprüfjobs erfolgreich abgeschlossen wurden, können Sie eine benutzerdefinierte Aufbewahrungsrichtlinie für das Repository einrichten.

Verwalten der Sicherheit

Der AppAssure Core kann Snapshot-Daten von Agenten im Repository verschlüsseln. Statt das gesamte Repository zu verschlüsseln, können Sie mit AppAssureeinen Verschlüsselungsschlüssel festlegen, wenn der Agent in einem Repository geschützt ist, sodass die Schlüssel für verschiedene Agenten wieder verwendet werden können. Durch die Verschlüsselung wird die Leistung nicht beeinträchtigt, da jeder aktive Verschlüsselungsschlüssel einen Verschlüsselungsbereich erstellt. Somit kann ein einzelner Core mehrere Nutzer unterstützen, indem mehrere Verschlüsselungsbereiche gehostet werden. In einer Umgebung mit mehreren Nutzern werden Daten in den Verschlüsselungsbereichen partitioniert und dedupliziert. Da Sie die Verschlüsselungsschlüssel verwalten, können die Schlüssel nicht durch den Verlust eines Volumes kompromittiert werden.

Wichtige Sicherheitskonzepte und -überlegungen sind u. a.:

- Die Verschlüsselung erfolgt mit 256-Bit-AES im CBC-Modus (Cipher Block Chaining), der mit SHA-3 kompatibel ist.
- Die Deduplizierung erfolgt innerhalb eines Verschlüsselungsbereichs, um den Datenschutz zu gewährleisten.
- Die Verschlüsselung wirkt sich nicht auf die Leistung aus.
- Sie können die im AppAssure Core konfigurierten Verschlüsselungsschlüssel hinzufügen, entfernen, importieren, exportieren, ändern und löschen.
- Sie können unbegrenzt viele Verschlüsselungsschlüssel auf dem Core erstellen.

Hinzufügen eines Verschlüsselungsschlüssels

Führen Sie die folgenden Schritte aus, um einen Verschlüsselungsschlüssel hinzuzufügen.

So fügen Sie einen Verschlüsselungsschlüssel hinzu

1 Navigieren Sie zum AppAssure Core, klicken Sie auf die Registerkarte „Konfiguration“ und wählen Sie dann **Sicherheit** aus.

Die Seite „Verschlüsselungsschlüssel“ wird angezeigt.

2 Wählen Sie im Dropdown-Menü „Aktionen“ **Verschlüsselungsschlüssel hinzufügen** aus.

Das Dialogfeld „Verschlüsselungsschlüssel erstellen“ wird angezeigt.

3 Geben Sie im Dialogfeld „Verschlüsselungsschlüssel erstellen“ die in der folgenden Tabelle beschriebenen Details für den Schlüssel ein.

Tabelle 15.

Textfeld	Beschreibung
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein.
Beschreibung	Geben Sie eine Anmerkung für den Verschlüsselungsschlüssel ein. Sie können so weitere Details für den Verschlüsselungsschlüssel angeben.
Passphrase	Geben Sie eine Passphrase ein. Diese wird für die Zugriffssteuerung verwendet.
Passphrase wiederholen	Geben Sie die Passphrase erneut ein. Dies wird zur Bestätigung der Passphraseneingabe verwendet.

4 Klicken Sie auf **OK**.

Das Dialogfeld wird geschlossen und der erstellte Verschlüsselungsschlüssel wird auf der Seite „Verschlüsselungsschlüssel“ angezeigt.

△ **VORSICHT: AppAssure verwendet 256-Bit-AES-Verschlüsselung im CBC-Modus (Cipher Block Chaining) mit 256-Bit-Schlüsseln. Obwohl die Verwendung der Verschlüsselung optional ist, wird von Dell dringend empfohlen, einen Verschlüsselungsschlüssel einzurichten und die festgelegte Passphrase zu schützen. Speichern Sie die Passphrase an einem sicheren Speicherort, da sie für die Datenwiederherstellung von entscheidender Bedeutung ist. Ohne Passphrase ist keine Datenwiederherstellung möglich.**

Bearbeiten eines Verschlüsselungsschlüssels

Führen Sie die folgenden Schritte aus, um Name oder Beschreibung eines vorhandenen Verschlüsselungsschlüssels zu bearbeiten.

So bearbeiten Sie einen Verschlüsselungsschlüssel

1 Navigieren Sie zum AppAssure Core, klicken Sie auf die Registerkarte „Konfiguration“ und wählen Sie dann **Sicherheit** aus.

Die Seite „Verschlüsselungsschlüssel“ wird angezeigt.

2 Wählen Sie im Dropdown-Menü „Konfiguration“ für den Verschlüsselungsschlüssel, der geändert werden soll, **Bearbeiten** aus.

Das Dialogfeld „Verschlüsselungsschlüssel bearbeiten“ wird angezeigt.

3 Bearbeiten Sie im Dialogfeld „Verschlüsselungsschlüssel bearbeiten“ den Namen oder die Beschreibung des Verschlüsselungsschlüssels und klicken Sie dann auf **OK**.

Das Dialogfeld wird geschlossen und die Änderungen des ausgewählten Verschlüsselungsschlüssels werden auf der Seite „Verschlüsselungsschlüssel“ angezeigt.

Ändern der Passphrase für einen Verschlüsselungsschlüssel

Führen Sie die nachstehend beschriebenen Schritte aus, um die Passphrase für einen Verschlüsselungsschlüssel zu ändern.

So ändern Sie die Passphrase für einen Verschlüsselungsschlüssel

1. Navigieren Sie zum AppAssure Core, klicken Sie auf die Registerkarte „Konfiguration“ und wählen Sie dann **Sicherheit** aus.

   Die Seite „Verschlüsselungsschlüssel“ wird angezeigt.

2. Wählen Sie im Dropdown-Menü „Konfiguration“ für den Verschlüsselungsschlüssel, der geändert werden soll, **Passphrase ändern** aus.

   Das Dialogfeld „Passphrase ändern“ wird angezeigt.

3. Geben Sie im Dialogfeld „Passphrase ändern“ die neue Passphrase für die Verschlüsselung ein, und wiederholen Sie die Passphrase, um sie zu bestätigen.

4. Klicken Sie auf **OK**.

   Das Dialogfeld wird geschlossen und die Passphrase wird aktualisiert.

△ **VORSICHT: AppAssure verwendet 256-Bit-AES-Verschlüsselung im CBC-Modus (Cipher Block Chaining) mit 256-Bit-Schlüsseln. Es wird empfohlen, dass Sie die festgelegte Passphrase sicher aufbewahren. Speichern Sie die Passphrase an einem sicheren Speicherort, da sie für die Datenwiederherstellung von entscheidender Bedeutung ist. Ohne Passphrase ist keine Datenwiederherstellung möglich.**

Importieren eines Verschlüsselungsschlüssels

Führen Sie die folgenden Schritte aus, um einen Verschlüsselungsschlüssel zu importieren.

So importieren Sie einen Verschlüsselungsschlüssel

1. Navigieren Sie zum AppAssure Core, klicken Sie auf die Registerkarte „Konfiguration“ und wählen Sie dann **Sicherheit** aus.

   Die Seite „Verschlüsselungsschlüssel“ wird angezeigt.

2. Wählen Sie im Dropdown-Menü „Aktionen“ **Importieren** aus.

   Das Dialogfeld „Schlüssel importieren“ wird angezeigt.

3. Klicken Sie im Dialogfeld „Schlüssel importieren“ auf **Durchsuchen**, um den Verschlüsselungsschlüssel zu suchen, der importiert werden soll, wählen Sie den Schlüssel aus, und klicken Sie auf **Öffnen**.

4. Klicken Sie im Dialogfeld „Schlüssel importieren“ auf **OK**.

   Das Dialogfeld wird geschlossen und der importierte Verschlüsselungsschlüssel wird auf der Seite „Verschlüsselungsschlüssel“ angezeigt.

Exportieren eines Verschlüsselungsschlüssels

Führen Sie die folgenden Schritte aus, um einen Verschlüsselungsschlüssel zu exportieren.

So exportieren Sie einen Verschlüsselungsschlüssel

1. Navigieren Sie zum AppAssure Core, klicken Sie auf die Registerkarte „Konfiguration“ und wählen Sie dann **Sicherheit** aus.

2 Wählen Sie im Dropdown-Menü „Konfiguration“ für den Verschlüsselungsschlüssel, der exportiert werden soll, **Export** aus.

   Das Dialogfeld „Schlüssel exportieren“ wird angezeigt.

3 Klicken Sie im Dialogfeld „Schlüssel exportieren“ auf **Datei speichern**, um die Verschlüsselungsschlüssel an einem sicheren Speicherort zu speichern, und klicken Sie auf **OK**.

Entfernen eines Verschlüsselungsschlüssels

Führen Sie die folgenden Schritte aus, um einen Verschlüsselungsschlüssel zu entfernen.

So entfernen Sie einen Verschlüsselungsschlüssel

1 Navigieren Sie zum AppAssure Core, klicken Sie auf die Registerkarte „Konfiguration“ und wählen Sie dann **Sicherheit** aus.

2 Wählen Sie im Dropdown-Menü „Konfiguration“ für den Verschlüsselungsschlüssel, der entfernt werden soll, **Entfernen** aus.

   Daraufhin wird eine Meldung mit der Bestätigung angezeigt, dass der Verschlüsselungsschlüssel entfernt wird.

3 Bestätigen Sie im Dialogfeld „Schlüssel entfernen“, dass der Verschlüsselungsschlüssel entfernt werden soll.

   HINWEIS: Durch das Entfernen eines Verschlüsselungsschlüssels werden die Daten nicht entschlüsselt.

   Das Dialogfeld wird geschlossen und der entfernte Verschlüsselungsschlüssel wird nicht mehr auf der Seite „Verschlüsselungsschlüssel“ angezeigt.

Verwalten von Cloud-Konten

Sie können in AppAssure 5 Links zu vorhandenen Anbietern von Cloud-Speicher festlegen. Nachdem Sie Ihre Anmeldeinformationen den Cloud-Einstellungen in der Core Console zugeordnet haben, können Sie Daten in der Cloud archivieren und archivierte Daten aus der Cloud importieren.

Informationen zur Verwaltung von Cloud-Konten in AppAssure 5 finden Sie in den folgenden Abschnitten:

- Hinzufügen eines Cloud-Kontos
- Bearbeiten eines Cloud-Kontos
- Konfigurieren von Cloud-Kontoeinstellungen
- Entfernen eines Cloud-Kontos

Hinzufügen eines Cloud-Kontos

Damit Sie archivierte Daten in eine Cloud archivieren können, müssen Sie die Kontoinformationen für den jeweiligen Cloud-Anbieter zur AppAssure Core Console hinzufügen. Führen Sie die nachstehend beschriebenen Schritte aus, um ein Cloud-Konto hinzuzufügen.

So fügen Sie ein Cloud-Konto hinzu

1 Wählen Sie in der AppAssure Core Console die Registerkarte „Extras“ aus.

2 Klicken Sie im linken Menü auf **Clouds**.

3 Klicken Sie auf der Seite „Clouds“ auf **Neues Konto hinzufügen**.

   Das Dialogfeld „Neues Konto hinzufügen“ wird geöffnet.

4 Wählen Sie in der Dropdown-Liste „Cloud-Typ“ einen kompatiblen Cloud-Anbieter aus.

5 Geben Sie abhängig vom Cloud-Typ, der in Schritt 4 ausgewählt wurde, die entsprechenden Details ein (siehe Beschreibung in der folgenden Tabelle).

Cloud-Typ	Textfeld	Beschreibung
Microsoft Azure	Speicherkontoname	Geben Sie den Namen Ihres Windows Azure-Speicherkontos ein.
	Zugriffsschlüssel	Geben Sie den Zugriffsschlüssel für Ihr Konto ein.
	Anzeigename	Geben Sie einen Anzeigenamen für dieses Konto in AppAssure ein, z. B. „Windows Azure 1“.
Amazon S3	Zugriffsschlüssel	Geben Sie den Zugriffsschlüssel für Ihr Cloud-Konto bei Amazon ein.
	Geheimer Schlüssel	Geben Sie den geheimen Schlüssel für dieses Konto ein.
	Anzeigename	Geben Sie einen Anzeigenamen für dieses Konto in AppAssure ein, z. B. „Amazon 1“.
Powered by OpenStack	Benutzername	Geben Sie den Benutzernamen für Ihr OpenStack-basiertes Cloud-Konto ein.
	API-Schlüssel	Geben Sie den API-Schlüssel für Ihr Konto ein.
	Anzeigename	Geben Sie einen Anzeigenamen für dieses Konto in AppAssure ein, z. B. „OpenStack 1“.
	Tenant-ID	Geben Sie Ihre Tenant-ID für dieses Konto ein.
	Authentifizierungs-URL	Geben Sie die Authentifizierungs-URL für dieses Konto ein.
Rackspace Cloud Block Storage	Benutzername	Geben Sie den Benutzernamen für Ihr Rackspace-Cloud-Konto ein.
	API-Schlüssel	Geben Sie den API-Schlüssel für dieses Konto ein.
	Anzeigename	Geben Sie einen Anzeigenamen für dieses Konto in AppAssure ein, z. B. „Rackspace 1“.

6 Klicken Sie auf **Hinzufügen**.

Das Dialogfeld wird geschlossen und das Konto wird auf der Seite „Clouds“ der Core Console angezeigt.

Bearbeiten eines Cloud-Kontos

Wenn Sie die Informationen für die Verbindung zu Ihrem Cloud-Konto ändern müssen, z. B. um das Kennwort zu ändern oder den Anzeigenamen zu ändern, können Sie dies in der Core Console auf der Registerkarte „Extras“ erledigen. Führen Sie die folgenden Schritte aus, um ein Cloud-Konto zu bearbeiten.

So bearbeiten Sie ein Cloud-Konto

1 Wählen Sie in der AppAssure Core Console die Registerkarte „Extras“ aus.

2 Klicken Sie im linken Menü auf **Clouds**.

3 Klicken Sie im Dropdown-Menü neben dem Cloud-Konto, das Sie bearbeiten möchten, auf **Bearbeiten**.

Das Fenster „Konto bearbeiten“ wird geöffnet.

4 Bearbeiten Sie die Details je nach Bedarf und klicken Sie dann auf **Speichern**.

HINWEIS: Sie können den Cloud-Typ nicht bearbeiten.

Konfigurieren von Cloud-Kontoeinstellungen

Über die Cloud-Konfigurationseinstellungen können Sie festlegen, wie oft AppAssure versuchen soll, eine Verbindung zum Cloud-Konto herzustellen, wie groß das zulässige Zeitlimit für diese Versuche sein soll. Führen Sie die folgenden Schritte aus, um die Verbindungseinstellungen für das Cloud-Konto zu konfigurieren.

So konfigurieren Sie Cloud-Kontoeinstellungen

1. Klicken Sie in der AppAssure Core Console auf die Registerkarte „Konfiguration“.
2. Klicken Sie im linken Menü auf **Einstellungen**.
3. Navigieren Sie auf der Seite „Einstellungen“ zu „Cloud-Configuration“.
4. Klicken Sie auf das Dropdown-Menü neben dem Cloud-Konto, das Sie konfigurieren möchten, und führen Sie dann eine der folgenden Aktionen durch:
   - Klicken Sie auf **Bearbeiten**.

     Das Dialogfeld „Cloud-Konfiguration“ wird angezeigt.

     a. Bearbeiten Sie mit den Aufwärts-/Abwärtspfeilen die Werte für die folgenden Optionen:
        - **Anforderungszeitlimit.** Dieser in Minuten und Sekunden angezeigte Wert bestimmt den zulässigen Zeitraum, in dem AppAssure versuchen soll, eine Verbindung zum Cloud-Konto herzustellen, wenn die Verbindung nicht sofort hergestellt wird. Die Verbindungsversuche werden nach dem eingegebenen Zeitraum eingestellt.
        - **Wiederholungsanzahl.** Dieser Wert gibt die Anzahl der Wiederholungsversuche an, die AppAssure durchführen soll, bevor ein festgelegt wird, dass das Cloud-Konto nicht erreicht werden kann.
        - **Größe des Schreibpuffers.** Gibt die Größe des Puffers an, der zum Schreiben archivierter Daten in die Cloud reserviert wird.
        - **Größe des Lesepuffers.** Gibt die Größe des Puffers an, der zum Lesen archivierter Daten aus der Cloud reserviert wird.

     b. Klicken Sie auf **Weiter**.
   - Klicken Sie auf **Zurücksetzen**.

     Die Konfiguration wird auf die folgenden Standardeinstellungen zurückgesetzt:
     - **Anforderungszeitlimit:** 01:30 (Minuten:Sekunden)
     - **Wiederholungsanzahl:** 3 (Versuche)

Entfernen eines Cloud-Kontos

Wenn Sie den Cloud-Dienst nicht mehr weiter nutzen oder für einen bestimmten Core nicht mehr nutzen möchten, können Sie das Cloud-Konto aus der Core Console entfernen. Führen Sie die folgenden Schritte aus, um ein Cloud-Konto zu entfernen.

So entfernen Sie ein Cloud-Konto

1. Wählen Sie in der AppAssure Core Console die Registerkarte „Extras“ aus.
2. Klicken Sie im linken Menü auf **Clouds**.
3. Klicken Sie im Dropdown-Menü neben dem Cloud-Konto, das Sie bearbeiten möchten, auf **Entfernen**.
4. Klicken Sie im Fenster „Konto löschen“ auf **Ja**, um zu bestätigen, dass das Konto gelöscht werden soll.
5. Wenn das Cloud-Konto derzeit verwendet wird, werden Sie in einem zweiten Fenster gefragt, ob das Konto dennoch entfernt werden soll. Klicken Sie zur Bestätigung auf **Ja**.

   HINWEIS: Wenn Sie ein Konto entfernen, das derzeit verwendet wird, schlagen alle für das betreffende Konto geplanten Archivierungsjobs fehl.

Informationen zur Replikation

Dieser Abschnitt enthält konzeptionelle und prozedurale Informationen, damit Sie wissen, wie die Replikation in AppAssure konfiguriert wird.

Als Replikation wird das Kopieren von Wiederherstellungspunkten und deren Übertragung auf einen sekundären Speicherort bezeichnet, um diese im Falle einer Notfallwiederherstellung verwenden zu können. Dazu ist eine gepaarte Quelle-Ziel-Beziehung zwischen zwei Cores erforderlich. Der Quell-Core kopiert die Wiederherstellungspunkte der geschützten Agenten und überträgt diese asynchron und laufend auf den Ziel-Core an einem Remote-Standort für die Notfallwiederherstellung. Der Remote-Standort kann ein unternehmenseigenes Datencenter (selbstverwalteter Core) oder ein MSP-Standort (Managed Service Provider) eines Drittanbieters oder eine Cloud-Umgebung sein. Bei der Replikation zu einem MSP können Sie integrierte Arbeitsabläufe verwenden, mit denen Sie Verbindungen anfordern und automatische Rückmeldungen erhalten können.

Mögliche Szenarien für die Replikation sind:

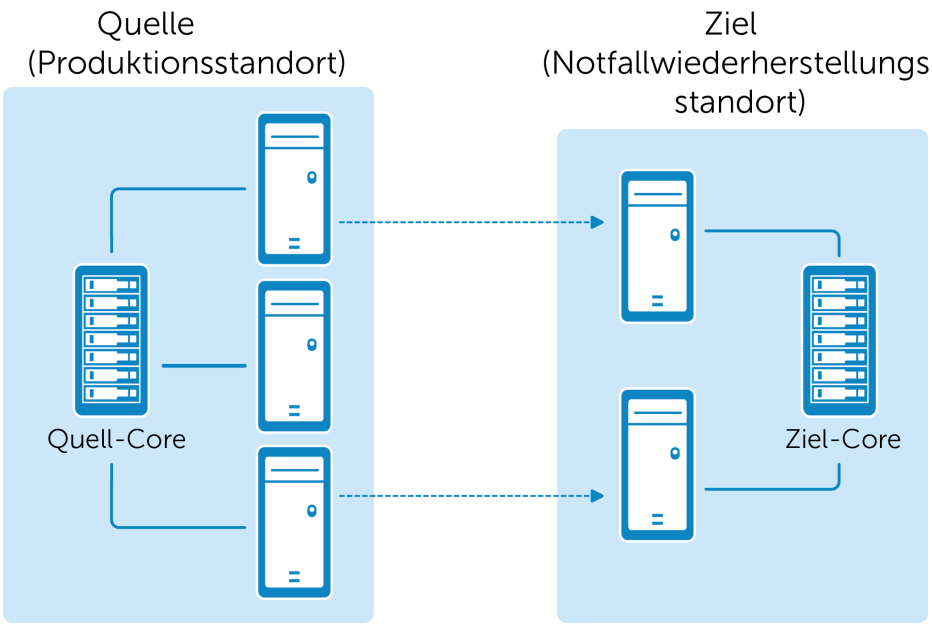
- **Replikation auf einen lokalen Speicherort.** Der Ziel-Core befindet sich in einem lokalen Rechenzentrum oder vor Ort und die Replikation wird jederzeit vorgenommen. In dieser Konfiguration ist eine Wiederherstellung auch möglich, wenn ein Core verloren geht.
- **Replikation auf einen externen Speicherort.** Der Ziel-Core befindet sich in einer externen Einrichtung zur Notfallwiederherstellung, um im Verlustfall eine Wiederherstellung zu ermöglichen.
- **Gegenseitige Replikation.** Zwei Rechenzentren an zwei unterschiedlichen Standorten enthalten jeweils einen Core, die Agenten schützen und gegenseitig als externe Sicherung für eine Notfallwiederherstellung dienen. In diesem Szenario repliziert jeder Core die Agenten auf den Core im anderen Rechenzentrum.
- **Gehostete Replikation und Cloud-Replikation.** AppAssure MSP-Partner unterhalten mehrere Ziel-Cores in einem Rechenzentrum oder in einer öffentlichen Cloud. Auf diesen Cores können Kunden des MSP-Partners gegen Gebühr Wiederherstellungspunkte von einem Quell-Core am Kundenstandort auf den Ziel-Core des MSPs replizieren.

> **HINWEIS:** In diesem Szenario haben Kunden nur Zugriff auf ihre eigenen Daten.

Mögliche Replikationskonfigurationen sind:

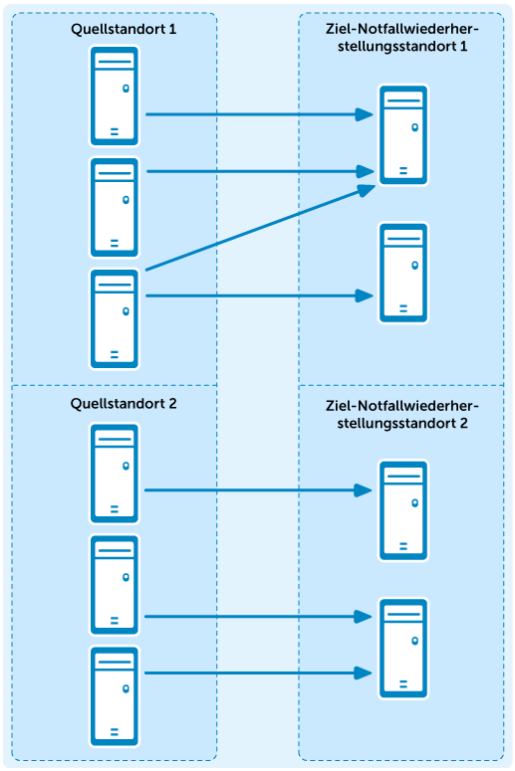
- **Punkt zu Punkt.** Ein einzelner Agent wird von einem einzelnen Quell-Core auf einen einzelnen Ziel-Core repliziert.

Abbildung 4. Punkt-zu-Punkt-Konfiguration



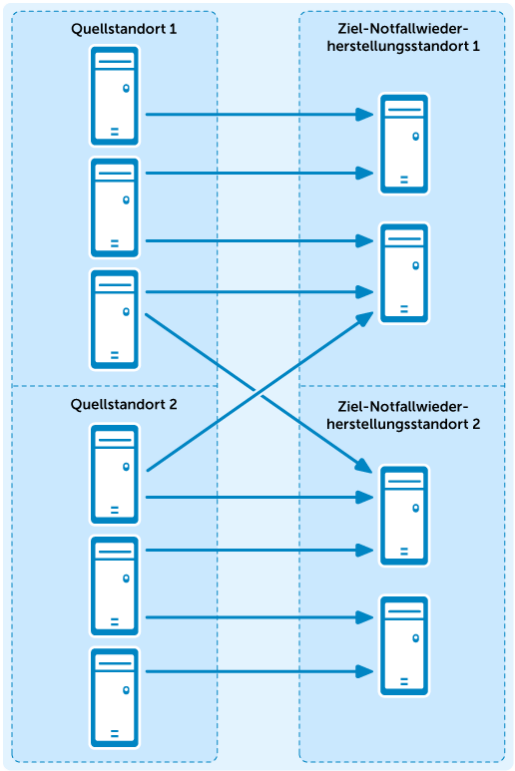
- **Mehrpunkt zu Punkt.** Agenten werden von mehreren Quell-Cores auf einen einzelnen Ziel-Core repliziert.

Abbildung 5. Mehrpunkt-zu-Punkt-Konfiguration



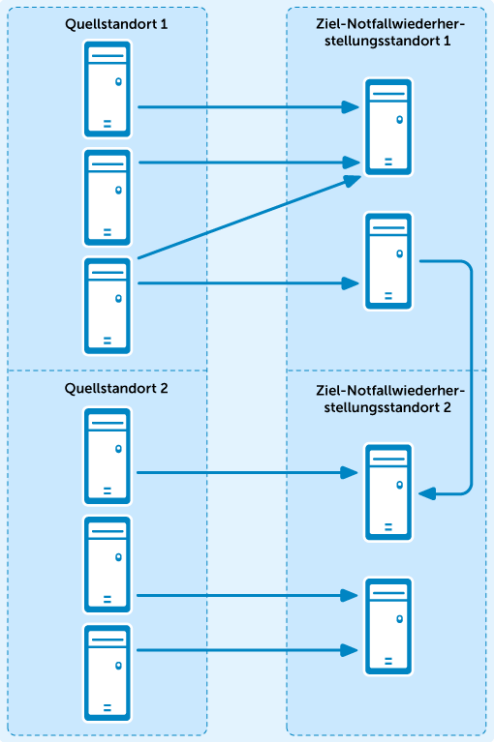
- **Punkt zu Mehrpunkt.** Ein Agent wird von einem einzelnen Quell-Core auf mehrere Ziel-Cores repliziert.

Abbildung 6. Punkt-zu-Mehrpunkt-Konfiguration



- **Multi-Hop.** Ein replizierter Agent wird von einem Ziel-Core auf einen anderen Ziel-Core repliziert, sodass eine zusätzliche Failover- bzw. Wiederherstellungsmöglichkeit entsteht.

Abbildung 7. Multi-Hop-Konfiguration



Informationen zum Seeding

Die Replikation beginnt mit dem Seeding: Die Erstübertragung von deduplizierten Basisimages und inkrementellen Snapshots von geschützten Agenten, die sich auf hunderte oder tausende Gigabytes an Daten summieren können. Die Anfangsreplikation kann durch Seeding der Anfangsdaten an den Ziel-Core über eine Netzwerkverbindung oder durch Erstellen und Speichern eines Seed-Laufwerks auf einem externen Medium und Transport an den Ziel-Core durchgeführt werden. Üblicherweise ist das Seed-Laufwerk bei umfangreichen Daten oder Standorten mit langsamer Verbindung nützlich.

HINWEIS: Es ist zwar möglich, das Seeding der Basisdaten über eine Netzwerkverbindung durchzuführen, dies wird jedoch nicht empfohlen. Beim ersten Seeding müssen u. U. sehr viele Daten übertragen werden, sodass eine normale WAN-Verbindung überlastet wird. Wenn die Seed-Daten zum Beispiel 10 GB umfassen und die WAN-Verbindung 24 MBit/s übertragen kann, dauert die Übertragung ungefähr eine Stunde.

Die Daten im Seeding-Archiv werden komprimiert, optional verschlüsselt und dedupliziert. Wenn die Gesamtgröße des Archivs den auf dem Wechseldatenträger verfügbaren Speicherplatz überschreitet, kann sich das Archiv, je nach verfügbarem Speicherplatz auf dem Datenträger, über mehrere Geräte erstrecken. Nachdem die Replikation eingerichtet wurde, werden alle Wiederherstellungspunkte, die nach der Einrichtung des Seed-Laufwerks erstellt wurden, vor der Übertragung der archivierten Daten an den Zielstandort repliziert. Beim Konsumieren des Seed-Laufwerks werden die archivierten Daten mit den replizierten Wiederherstellungspunkten synchronisiert, die im Repository auf dem Ziel-Core vorhanden sind.

Seeding ist ein zweistufiger Prozess (auch als Kopieren-Konsumieren bezeichnet):

- Der erste Schritt ist das Kopieren. Dabei werden die Anfangsdaten für die Replikation auf einen Wechseldatenträger geschrieben. Es gibt zwei Kopiermöglichkeiten: Duplizieren der noch nicht replizierten Wiederherstellungspunkte vom Quell-Core auf ein lokales Wechselmedium, z. B. ein USB-Laufwerk, oder Duplizieren aller vorhandenen Wiederherstellungspunkte (Option „Wiederherstellungspunktkette erstellen (Waisen korrigieren)“). Nachdem dem Kopieren muss der

Datenträger dann vom Standort des Quell-Core zum Remote-Standort des Ziel-Core transportiert werden.

- Der zweite Teil ist das Konsumieren. Dabei werden die replizierten Daten auf dem transportierten Datenträger in das Repository des Ziel-Core kopiert. Der Ziel-Core konsumiert die Wiederherstellungspunkten und bildet dann daraus die replizierten Agenten.

  HINWEIS: Während die Replikation von inkrementellen Snapshots zwischen Quell- und Ziel-Cores erfolgen kann, bevor ein Seeding durchgeführt wurde, bleiben die replizierten Snapshots, die von der Quelle an das Ziel übertragen werden, solange „verwaist“, bis die Anfangsdaten konsumiert und mit den replizierten Basisimages kombiniert wurden. Weitere Informationen zu verwaisten Wiederherstellungspunkten finden Sie unter Löschen einer verwaisten Wiederherstellungspunktkette.

Da große Datenmengen auf den Wechseldatenträger kopiert werden müssen, wird eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung zum Wechseldatenträger empfohlen.

Informationen zu Failover und Failback in AppAssure

Im Fall eines schwerwiegenden Ausfalls, bei dem Quell-Core und Agenten nicht verfügbar sind, unterstützt AppAssure in replizierten Umgebungen Failover und Failback. Failover bezeichnet das Umschalten auf einen redundanten oder Standby-Ziel-AppAssure-Core bei einem Systemausfall oder bei einer anormalen Beendigung von Quell-Core und zugehörigen Agenten. Das Hauptziel des Failovers besteht darin, einen neuen Agenten zu starten, der mit dem ausgefallenen Agenten identisch ist, der vom ausgefallenen Ziel-Core geschützt wurde. Das zweite Ziel besteht darin, den Ziel-Core in einen neuen Modus zu schalten, sodass der Ziel-Core den Failover-Agenten genauso schützt, wie der Quell-Core den ursprünglichen Agenten vor dem Ausfall geschützt hat. Der Ziel-Core kann am sekundären Standort Instanzen aus replizierten Agenten wiederherstellen und sofort den Schutz auf den Failover-Maschinen übernehmen.

Failback bezeichnet das Wiederherstellen eines Agenten und eines Core im ursprünglichen Zustand (vor dem Ausfall). Das Hauptziel des Failbacks besteht darin, den Agenten (in den meisten Fällen eine neue Maschine, die den ausgefallenen Agenten ersetzt) in einen solchen Zustand wiederherzustellen, der mit dem letzten Zustand des neuen, temporären Agenten identisch ist. Nach der Wiederherstellung wird der Agent durch einen wiederhergestellten Quell-Core geschützt. Die Replikation wird ebenfalls wiederhergestellt und der Ziel-Core fungiert wieder als Replikationsziel. Weitere Informationen finden Sie unter Anleitung für Failover und Failback.

Informationen zu Replikation und verschlüsselten Wiederherstellungspunkten

Das Seed-Laufwerk enthält keine Sicherungen der Registrierung und Zertifikate des Quell-Core. Es enthält allerdings die Verschlüsselungsschlüssel des Quell-Core, wenn die Wiederherstellungspunkte, die vom Quell- zum Ziel-Core repliziert werden, verschlüsselt sind. Die replizierten Wiederherstellungspunkte bleiben verschlüsselt, nachdem sie auf den Ziel-Core übertragen wurden. Die Besitzer oder Administratoren des Ziel-Core benötigen die Passphrase, um die verschlüsselten Daten wiederherzustellen.

Informationen zu Aufbewahrungsrichtlinien für die Replikation

Die Aufbewahrungsrichtlinien auf dem Quell- und dem Ziel-Core werden nicht synchronisiert. Rollup und Ad-hoc-Löschung werden auf jedem Core unmittelbar nach der Einrichtung sowie im Rahmen der nächtlichen Jobs unabhängig voneinander durchgeführt.

Weitere Informationen zu Aufbewahrungsrichtlinien finden Sie unter Verwalten von Aufbewahrungsrichtlinien.

Überlegungen zur Übertragungsleistung für Replikationsdaten

Wenn die Bandbreite zwischen Quell- und Ziel-Core für die Übertragung der gespeicherten Wiederherstellungspunkten nicht ausreicht, erfolgt bei der Replikation zuerst ein Seeding des Ziel-Core mit Basisimages und Wiederherstellungspunkten der ausgewählten Server, die im Quell-Core geschützt werden. Der Seeding-Prozess kann jederzeit durchgeführt werden - im Rahmen der Erstübertragung von Daten als Grundlage für die regelmäßig geplante Replikation bzw. bei einer erneuten Aktivierung der Replikation für eine zuvor replizierte Maschine, deren Replikation vorübergehend oder komplett deaktiviert wurde. In diesem Fall können Sie mit der Option „Wiederherstellungspunktkette erstellen (Waisen korrigieren)“ noch nicht replizierte Wiederherstellungspunkte auf ein Seed-Laufwerk replizieren.

Der der Vorbereitung der Replikation müssen Sie die folgenden Faktoren beachten:

- **Änderungsrate.** Die Änderungsrate ist die Rate, mit der sich der Umfang der geschützten Daten vergrößert. Die Rate hängt vom Datenvolumen ab, das auf geschützten Volumes geändert wird und vom Schutzintervall der Volumes. Wenn mehrere Blöcke im Volume geändert werden, wird durch Verringerung des Schutzintervalls auch die Änderungsrate reduziert.
- **Bandbreite.** Die Bandbreite ist die verfügbare Übertragungsgeschwindigkeit zwischen dem Quell-Core und dem Ziel-Core. Die Bandbreite muss unbedingt größer als die Änderungsrate sein, damit die Replikation mit den Wiederherstellungspunkten Schritt halten kann, die im Rahmen der Snapshots erstellt werden. Aufgrund der zwischen den Cores übertragenen Datenmenge sind eventuell mehrere parallele Streams mit Leitungsgeschwindigkeit erforderlich, um die Geschwindigkeit einer 1-GB-Ethernetverbindung zu erreichen.

  HINWEIS: Die vom Internetdienstanbieter angegebene Bandbreite ist die verfügbare Gesamtbandbreite. Die ausgehende Bandbreite wird auf alle Geräten im Netzwerk aufgeteilt. Es muss sichergestellt sein, dass für die Replikation ausreichend freie Bandbreite für die Änderungsrate zur Verfügung steht.

- **Anzahl der Agenten.** Weiterhin muss die Anzahl der Agenten berücksichtigt werden, die pro Quell-Core geschützt werden und wie viele davon auf den Ziel-Core repliziert werden sollen. Mit AppAssure können Sie die Replikation für jeden geschützten Server einzeln durchführen, sodass nur bestimmte Server repliziert werden. Wenn alle geschützten Server repliziert werden müssen, wirkt sich dies erheblich auf die Änderungsrate aus, insbesondere, wenn die Bandbreite zwischen Quell- und Ziel-Cores für Umfang und Größe der replizierten Wiederherstellungspunkte unzureichend ist.

Abhängig von der Netzwerkkonfiguration kann die Replikation ein zeitaufwendiger Vorgang sein.

Die folgende Tabelle „Maximale Änderungsrate für WAN-Verbindungstypen“ enthält einige Beispiele für die erforderliche Bandbreite pro Gigabyte für eine zumutbare Änderungsrate.

Tabelle 16.

WAN-Typ	Bandbreite	Max. Änderungsrate
DSL	768 KBit/s und mehr	330 MB pro Stunde
Kabel	1 MBit/s und mehr	429 MB pro Stunde
T1	1,5 MBit/s und mehr	644 MB pro Stunde
Glasfaser	20 MBit/s und mehr	8,38 GB pro Stunde

HINWEIS: Um optimale Ergebnisse zu erhalten, sollten Sie die in der obigen Tabelle aufgeführten Empfehlungen einhalten.

Bei einem Verbindungsausfall während der Datenübertragung wird die Replikation vom letzten Fehlerpunkt der Übertragung wieder aufgenommen, nachdem die Verbindung wieder funktionsfähig ist.

Anleitung für die Einrichtung der Replikation

Um Daten mit AppAssure zu replizieren, müssen Sie den Quell-Core und den Ziel-Core für die Replikation konfigurieren. Nachdem die Replikation konfiguriert wurde, können Sie Agentendaten replizieren, die Replikation überwachen und verwalten sowie Wiederherstellungen durchführen.

Die Durchführung von Replikationen in AppAssure umfasst die folgenden Vorgänge:

- **Einrichten eines Repositorys auf dem Ziel-Core.** Weitere Informationen zum Hinzufügen eines Repositorys zum Ziel-Core finden Sie unter Erstellen eines Repositorys.
- **Konfigurieren der selbstverwalteten Replikation.** Weitere Informationen zur Replikation auf einen selbstverwalteten Ziel-Core finden Sie unter Replikation auf einen selbstverwalteten Ziel-Core.
- **Konfigurieren der Replikation zu einem externen Anbieter.** Weitere Informationen zur Replikation auf den Ziel-Core eines externen Anbieters finden Sie unter Replikation auf den Ziel-Core eines externen Anbieters.
- **Replikation eines vorhandenen Agenten.** Weitere Informationen zum Replizieren eines Agenten, der bereits vom Quell-Core geschützt wird, finden Sie unter Hinzufügen einer Maschine zu einer bestehenden Replikation.
- **Konsumieren des Seed-Laufwerks.** Weitere Informationen zum Konsumieren der Seed-Laufwerksdaten auf dem Ziel-Core finden Sie unter Konsumieren des Seed-Laufwerks auf einem Ziel-Core.
- **Festlegen der Replikationspriorität für einen Agenten.** Weitere Informationen zum Priorisieren der Replikation von Agenten finden Sie unter Festlegen der Replikationspriorität für einen Agenten.
- **Festlegen eines Replikationszeitplans für einen Agenten.** Weitere Informationen zum Festlegen eines Replikationszeitplans finden Sie unter Planen der Replikation.
- **Bedarfsabhängige Überwachung der Replikation.** Weitere Informationen zur Überwachung der Replikation finden Sie unter Überwachen der Replikation.
- **Bedarfsabhängige Verwaltung der Replikationseinstellungen.** Weitere Informationen zur Verwaltung der Replikationseinstellungen finden Sie unter Verwalten der Replikationseinstellungen.
- **Wiederherstellen replizierter Daten im Notfall oder bei Datenverlust.** Weitere Informationen zur Wiederherstellung replizierter Daten finden Sie unter Wiederherstellen von replizierten Daten.

Replikation auf einen selbstverwalteten Ziel-Core

Bein einem selbstverwalteten Core handelt es sich um einen Core, auf den Sie direkten Zugriff haben. Diese werden oftmals von Unternehmen an einem externen Standort unterhalten. Die Replikation kann vollständig im Quell-Core erledigt werden (sofern kein Daten-Seeding notwendig ist). Bei einem Seeding müssen Sie das Seed-Laufwerk auf dem Ziel-Core konsumieren, nachdem die Replikation auf dem Quell-Core konfiguriert wurde.

HINWEIS: Diese Konfiguration gilt für die Replikation an einen externen Standort sowie für die gegenseitige Replikation. Der AppAssure Core muss auf allen Quell- und Zielmaschinen installiert sein. Wenn Sie AppAssure für eine Mehrpunkt-zu-Punkt Replikation konfigurieren, müssen Sie diese Aufgabe auf allen Quell-Cores sowie auf einem Ziel-Core ausführen.

Führen Sie die folgenden Schritte aus, um den Quell-Core für die Replikation auf einen selbstverwalteten Ziel-Core zu konfigurieren.

So führen Sie eine Replikation auf einen selbstverwalteten Ziel-Core durch

1. Navigieren Sie zur AppAssure Core Console und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.
2. Klicken Sie auf der Seite „Replikation“ auf **Ziel-Core hinzufügen**.

   Der Replikationsassistent wird geöffnet.

3 Wählen Sie auf der Seite „Ziel-Core“ des Replikationsassistenten **Ich verfüge über einen eigenen Ziel-Core** und geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

> **HINWEIS:** Mit AppAssure 5 können Sie eine Replikation auf Dell DL-4000-Systeme durchführen. Informationen hierzu finden Sie in den *Dell AppAssure 5 Releaseinformationen* bzw. in der AppAssure 5 Knowledge Base.

Tabelle 17.

Textfeld	Beschreibung
Hostname	Geben Sie den Hostnamen oder die IP-Adresse der Core-Maschine ein, auf die Daten repliziert werden.
Port	Geben Sie die Portnummer ein, über die der AppAssure Core mit der Maschine kommuniziert. Die Standardportnummer ist *8006*.
Benutzername	Geben Sie den Benutzernamen für den Zugriff auf den Core ein.
Kennwort	Geben Sie das Kennwort für den Zugriff auf den Core ein.

- Wenn der Core, der hinzugefügt werden soll, zuvor mit diesem Quell-Core gepaart wurde, können Sie wie folgt vorgehen:
  a Wählen Sie **Vorhandenen Ziel-Core verwenden** aus.
  b Wählen Sie den Ziel-Core in der Dropdown-Liste aus.
  c Klicken Sie auf **Weiter**.
  d Gehen Sie zu Schritt 7.

4 Klicken Sie auf **Weiter**.

> **HINWEIS:** Wenn auf dem Ziel-Core kein Repository vorhanden ist, wird eine Warnung mit dem Hinweis angezeigt, dass Sie den Quell-Core zwar mit dem Ziel-Core paaren können, Agenten aber erst dorthin replizieren können, nachdem ein Repository eingerichtet wurde. Informationen zum Einrichten eines Repositorys auf einem Core finden Sie unter Erstellen eines Repositorys.

5 Geben Sie auf der Seite „Details“ einen Namen für diese Replikationskonfiguration ein, z. B. SourceCore1.

- Wählen Sie **Mein Core wurde migriert und ich möchte die Replikation reparieren** aus, wenn Sie eine frühere Replikationskonfiguration wieder aktivieren oder reparieren.

6 Klicken Sie auf **Weiter**.

7 Wählen Sie auf der Seite „Agenten“ die Agenten aus, die repliziert werden sollen, und wählen Sie in den Dropdown-Listen in der Spalte „Repository“ ein Repository für jeden Agenten aus.

8 Führen Sie die folgenden Schritte aus, wenn Sie ein Seeding für die Übertragung der Basisdaten durchführen möchten:

> **HINWEIS:** Da große Datenmengen auf den Wechseldatenträger kopiert werden müssen, wird eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung zum Wechseldatenträger empfohlen.

a Wählen Sie auf der Seite „Agenten“ *Seed-Laufwerk für anfängliche Übertragung verwenden* aus.
   - Wenn derzeit Agenten auf einen Ziel-Core replizieren, können Sie diese Agenten in das Seed-Laufwerk einbeziehen, indem Sie **Mit bereits replizierten** auswählen.

b Klicken Sie auf **Weiter**.

c Wählen Sie auf der Seite „Seed-Laufwerkspeicherort“ in der Dropdown-Liste **Typ des Speicherorts** einen der folgenden Zieltypen aus:
   - Lokal

- Netzwerk
- Cloud

d Geben Sie abhängig vom Typ des Speicherorts, der in Schritt c ausgewählt wurde, die Details für das Archiv ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 18.

Option	Textfeld	Beschreibung
Lokal	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. D:\Arbeit\Archiv.
Netzwerk	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. \\Servername\Freigabename.
	Benutzername	Geben Sie einen Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **HINWEIS:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname ist „AppAssure-5-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

e Klicken Sie auf **Weiter**.

f Geben Sie auf der Seite „Seed-Laufwerkoptionen“ die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 19.

Element	Beschreibung
Maximale Größe	Umfangreiche Datenarchive können in mehrere Segmente aufgeteilt werden. Wählen Sie die maximale Größe des Segments aus, die zum Erstellen des Seed-Laufwerks reserviert werden soll. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie **Gesamtes Ziel** aus, um den gesamten verfügbaren Speicherplatz im Pfad, der auf der Seite „Seed-Laufwerkspeicherort“ angegeben wurde, für die zukünftige Verwendung zu reservieren. (Wenn beispielsweise „D:\Arbeit\Archiv“ als Speicherort angegeben wurde, wird der gesamte verfügbare Speicherplatz auf dem Laufwerk D: ggf. für das Kopieren des Seed-Laufwerks reserviert, aber nicht unmittelbar nach Beginn des Kopiervorgangs.) • Geben Sie in das leere Textfeld einen Wert ein und wählen Sie dann eine Maßeinheit in der Dropdown-Liste aus, um den maximal reservierten Speicherplatz festzulegen.
Kunden-ID (optional)	Geben Sie die Kundennummer ein, die vom Dienstanbieter zugewiesen wurde (optional).

Tabelle 19.

Element	Beschreibung
Recyclingaktion	Falls der Pfad bereits ein Seed-Laufwerk enthält, wählen Sie eine der folgenden Optionen aus: • **Nicht wiederverwenden.** Vorhandene Seed-Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, können keine Daten in das Seed-Laufwerk geschrieben werden. • **Diesen Core ersetzen.** Alle bereits vorhandenen Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert. • **Vollständig löschen.** Alle Seed-Daten werden aus dem Verzeichnis gelöscht, bevor das Seed-Laufwerk geschrieben wird.
Anmerkung	Geben Sie eine Anmerkung ein, die das Seed-Laufwerk beschreibt.
Alle Agenten zum Seed-Laufwerk hinzufügen	Wählen Sie diese Option aus, um alle Agenten im Quell-Core mit dem Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt.
Wiederherstellungspunktkette erstellen (Waisen korrigieren)	Wählen Sie diese Option aus, um die gesamte Wiederherstellungspunktkette auf das Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt. **HINWEIS:** Beim Seeding in AppAssure 5.4 werden normalerweise nur die letzten Wiederherstellungspunkte auf das Seed-Laufwerk repliziert, um Zeitaufwand und Speicherplatz zum Erstellen des Seed-Laufwerks zu verringern. Wenn Wiederherstellungspunktketten auf dem Seed-Laufwerk erstellt werden sollen, muss auf dem Seed-Laufwerk genügend Speicherplatz zum Speichern der letzten Wiederherstellungspunkte der angegebenen Agenten vorhanden sein. Dieser Vorgang kann entsprechend länger dauern.
Kompatibles Format verwenden	Wählen Sie diese Option aus, um das Seed-Laufwerk in einem Format zu erstellen, das mit der neuen Version und älteren Versionen des AppAssure Core kompatibel ist. **HINWEIS:** Das aktuelle Seed-Laufwerksformat ist nicht kompatibel mit 5.3-Versionen des Core. Archive, die in AppAssure 5.3 erstellt wurden, sind mit AppAssure 5.4 kompatibel.

g Führen Sie eine der folgenden Aktionen aus:

- Klicken Sie auf **Weiter**, wenn das Kontrollkästchen **Alle Agenten zum Seed-Laufwerk hinzufügen** deaktiviert wurde.
- Wechseln Sie zu Schritt 9, wenn **Alle Agenten zum Seed-Laufwerk hinzufügen** aktiviert wurde.

h Wählen Sie auf der Seite „Agenten“ die Agenten aus, die mit dem Seed-Laufwerk auf den Ziel-Core repliziert werden sollen.

9 Klicken Sie auf **Finish**.

10 Transportieren Sie ggf. das erstellte Seed-Laufwerk zum Ziel-Core.

Damit ist die Paarung von Quell-Core und Ziel-Core abgeschlossen. Die Replikation beginnt. Dabei entstehen jedoch verwaiste Wiederherstellungspunkte im Ziel-Core, bis das Seed-Laufwerk mit den erforderlichen Basisimages konsumiert wurde.

Replikation auf den Ziel-Core eines externen Anbieters

Bei einem Core eines externen Anbieters handelt es sich um einen Ziel-Core, der von einem MSP unterhalten und verwaltet wird. Für eine Replikation auf einen Core, der von einem externen Anbieter verwaltet wird, muss der Kunden keinen Zugriff auf den Ziel-Core haben.

Bei der Replikation auf den Core eines externen Anbieters müssen vom Kunden und vom externen Anbieter bestimmte Aufgaben ausgeführt werden. Nachdem ein Kunde eine Replikationsanforderung für einen Quell-Core gesendet hat, muss der MSP die Konfiguration im Ziel-Core vornehmen, indem er die Anforderung überprüft.

HINWEIS: Diese Konfiguration gilt für gehostete und Cloud-Replikation. Der AppAssure Core muss auf allen Quell-Core-Maschinen installiert sein. Wenn Sie AppAssure für eine Mehrpunkt-zu-Punkt Replikation konfigurieren, müssen Sie diese Aufgabe auf allen Quell-Cores ausführen.

Sie müssen die folgenden Aufgaben ausführen, um Daten auf einen Ziel-Core zu replizieren, der von einem externen Anbieter verwaltet wird:

1 Senden einer Replikationsanforderung an einen externen Dienstanbieter

2 Überprüfen einer Replikationsanforderung von einem Kunden oder Ignorieren einer Replikationsanforderung von einem Kunden

Senden einer Replikationsanforderung an einen externen Dienstanbieter

Führen Sie als Endbenutzer, der einen Core abonniert hat, der extern verwaltet wird, z. B. durch einen MSP, die nachstehend aufgeführten Schritte aus, um eine Replikationsanforderung an den externen Dienstanbieter zu senden.

So senden Sie eine Replikationsanforderung an einen externen Dienstanbieter

1 Navigieren Sie zur AppAssure Core Console und klicken Sie auf die Registerkarte „Replikation“ oder das Replikationssymbol in der linken Spalte.

2 Klicken Sie auf der Seite „Replikation“ auf **Ziel-Core hinzufügen**.

Der Replikationsassistent wird geöffnet.

3 Wählen Sie auf der Seite „Ziel-Core“ des Replikationsassistenten **Ich habe ein Abonnement bei einem Drittanbieter für Offsite-Sicherungs- und Notfallwiederherstellungsdienste** und geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 20.

Textfeld	Beschreibung
Hostname	Geben Sie den Hostnamen, die IP-Adresse oder FQDN für die externe Core-Maschine ein.
Port	Geben Sie die Portnummer ein, die Sie vom externen Dienstanbieter erhalten haben. Die Standardportnummer ist *8006*.

- Wenn der Core, der hinzugefügt werden soll, zuvor mit diesem Quell-Core gepaart wurde, können Sie wie folgt vorgehen:

  a Wählen Sie **Vorhandenen Ziel-Core verwenden** aus.

  b Wählen Sie den Ziel-Core in der Dropdown-Liste aus.

  c Klicken Sie auf **Weiter**.

  d Gehen Sie zu Schritt 7.

4 Klicken Sie auf **Weiter**.

5 Geben Sie auf der Seite „Details“ die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 21.

Textfeld	Beschreibung
E-Mail-Adresse	Geben Sie die E-Mail-Adresse für das Abonnement des externen Dienstes an.
Kunden-ID (optional)	Geben Sie die Kundennummer ein, die vom Dienstanbieter zugewiesen wurde (optional).

6 Klicken Sie auf **Weiter**.

7 Wählen Sie auf der Seite „Agenten“ die Agenten aus, die auf den externen Core repliziert werden sollen.

8 Führen Sie die folgenden Schritte aus, wenn Sie ein Seeding für die Übertragung der Basisdaten durchführen möchten:

> **HINWEIS:** Da große Datenmengen auf den Wechseldatenträger kopiert werden müssen, wird eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung zum Wechseldatenträger empfohlen.

a Wählen Sie auf der Seite „Agenten“ *Seed-Laufwerk für anfängliche Übertragung verwenden* aus.

- Wenn derzeit Agenten auf einen Ziel-Core replizieren, können Sie diese Agenten in das Seed-Laufwerk einbeziehen, indem Sie **Mit bereits replizierten** auswählen.

b Klicken Sie auf **Weiter**.

c Wählen Sie auf der Seite „Seed-Laufwerkspeicherort“ in der Dropdown-Liste **Typ des Speicherorts** einen der folgenden Zieltypen aus:

- Lokal
- Netzwerk
- Cloud

d Geben Sie abhängig vom Typ des Speicherorts, der in Schritt c ausgewählt wurde, die Details für das Archiv ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 22.

Option	Textfeld	Beschreibung
Lokal	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. D:\Arbeit\Archiv.
Netzwerk	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. \\Servername\Freigabename.
	Benutzername	Geben Sie einen Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.

Tabelle 22.

Option	Textfeld	Beschreibung
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **HINWEIS:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname ist „AppAssure-5-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

e Klicken Sie auf **Weiter**.

f Geben Sie auf der Seite „Seed-Laufwerkoptionen“ die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 23.

Element	Beschreibung
Maximale Größe	Umfangreiche Datenarchive können in mehrere Segmente aufgeteilt werden. Wählen Sie den maximalen Speicherplatz aus, der zum Erstellen des Seed-Laufwerks reserviert werden soll. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie **Gesamtes Ziel** aus, um den gesamten verfügbaren Speicherplatz im Pfad, der auf der Seite „Seed-Laufwerkspeicherort“ angegeben wurde, zu reservieren. (Wenn beispielsweise „D:\Arbeit\Archiv“ als Speicherort angegeben wurde, wird der gesamte verfügbare Speicherplatz auf dem Laufwerk D: reserviert.) • Geben Sie in das leere Textfeld einen Wert ein und wählen Sie dann eine Maßeinheit in der Dropdown-Liste aus, um den maximal reservierten Speicherplatz festzulegen.
Kunden-ID (optional)	Geben Sie die Kundennummer ein, die vom Dienstanbieter zugewiesen wurde (optional).
Recyclingaktion	Falls der Pfad bereits ein Seed-Laufwerk enthält, wählen Sie eine der folgenden Optionen aus: • **Nicht wiederverwenden.** Vorhandene Seed-Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, können keine Daten in das Seed-Laufwerk geschrieben werden. • **Diesen Core ersetzen.** Alle bereits vorhandenen Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert. • **Vollständig löschen.** Alle Seed-Daten werden aus dem Verzeichnis gelöscht, bevor das Seed-Laufwerk geschrieben wird.
Anmerkung	Geben Sie eine Anmerkung ein, die das Seed-Laufwerk beschreibt.
Alle Agenten zum Seed-Laufwerk hinzufügen	Wählen Sie diese Option aus, um alle Agenten im Quell-Core mit dem Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt.

Tabelle 23.

Element	Beschreibung
Wiederherstellungspunktkette erstellen (Waisen korrigieren)	Wählen Sie diese Option aus, um die gesamte Wiederherstellungspunktkette auf das Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt. **HINWEIS:** Beim Seeding in AppAssure 5.4 werden normalerweise nur die letzten Wiederherstellungspunkte auf das Seed-Laufwerk repliziert, um Zeitaufwand und Speicherplatz zum Erstellen des Seed-Laufwerks zu verringern. Wenn Wiederherstellungspunktketten auf dem Seed-Laufwerk erstellt werden sollen, muss auf dem Seed-Laufwerk genügend Speicherplatz zum Speichern der letzten Wiederherstellungspunkte der angegebenen Agenten vorhanden sein. Dieser Vorgang kann entsprechend länger dauern.
Kompatibles Format verwenden	Wählen Sie diese Option aus, um das Seed-Laufwerk in einem Format zu erstellen, das mit der neuen Version und älteren Versionen des AppAssure Core kompatibel ist. **HINWEIS:** Das aktuelle Seed-Laufwerksformat ist nicht kompatibel mit 5.3-Versionen des Core. Archive, die in AppAssure 5.3 erstellt wurden, sind mit AppAssure 5.4 kompatibel.

g Führen Sie eine der folgenden Aktionen aus:

- Klicken Sie auf **Weiter**, wenn das Kontrollkästchen **Alle Agenten zum Seed-Laufwerk hinzufügen** deaktiviert wurde.
- Wechseln Sie zu Schritt 9, wenn **Alle Agenten zum Seed-Laufwerk hinzufügen** aktiviert wurde.

h Wählen Sie auf der Seite „Agenten“ die Agenten aus, die mit dem Seed-Laufwerk auf den Ziel-Core repliziert werden sollen.

9 Klicken Sie auf **Finish**.

10 Senden Sie ggf. das erstellte Seed-Laufwerk an den externen Dienstanbieter. Befolgen Sie dazu dessen Anweisungen.

Überprüfen einer Replikationsanforderung von einem Kunden

Nachdem ein Benutzer die Schritte in Senden einer Replikationsanforderung an einen externen Dienstanbieter durchgeführt hat, wird von Quell-Core eine Replikationsanforderung an den externen Ziel-Core gesendet. Der externe Anbieter kann die Anforderung überprüfen und genehmigen, damit die Replikation für den Kunden durchgeführt wird, oder die Anforderung ablehnen, sodass keine Replikation stattfindet.

Wählen Sie eine der folgenden Optionen aus:

- Genehmigen einer Replikationsanforderung
- Ablehnen einer Replikationsanforderung

Genehmigen einer Replikationsanforderung

Führen Sie die folgenden Schritte aus, um eine Replikationsanforderung auf einem externen Ziel-Core zu genehmigen.

So genehmigen Sie eine Replikationsanforderung

1 Öffnen Sie auf dem Ziel-Core die AppAssure Core Console und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.

2 Klicken Sie auf der Seite „Replikation“ auf **Anstehende Anforderungen (Zahl)**.

Der Abschnitt „Anstehende Replikationsanforderungen“ wird angezeigt.

3 Klicken Sie unter „Anstehende Replikationsanforderungen“ auf das Dropdown-Menü neben der Anforderung, die überprüft werden soll, und klicken Sie dann auf **Überprüfen**.

Das Fenster „Replikationsanforderung überprüfen“ wird angezeigt.

> **HINWEIS:** Die im Abschnitt „Quell-Core-Identität“ dieses Fensters angezeigten Informationen stammen aus der Anforderung des Kunden.

4 Führen Sie unter „Quell-Core-Identität“ eine der folgenden Aktionen aus:

- Wählen Sie „Vorhandenen replizierten Core ersetzen“ und dann einen Core in der Dropdown-Liste aus.
- Wählen Sie „Neuen Quell-Core erstellen“ aus und überprüfen Sie dann, ob Core-Name, E-Mail-Adresse des Kunden und Kunden-ID richtig sind. Bearbeiten Sie ggf. die Informationen.

5 Wählen Sie unter „Agenten“ die Maschinen aus, für die die Genehmigung gilt, und wählen Sie in den Dropdown-Listen in der Spalte „Repository“ das entsprechende Repository für die einzelnen Agenten aus.

6 Geben Sie optional im Textfeld „Anmerkung“ eine Beschreibung oder Nachricht ein, die in die Antwort an den Kunden aufgenommen werden soll.

7 Klicken Sie auf **Antwort senden**.

Die Replikation wird akzeptiert.

Ablehnen einer Replikationsanforderung

Führen Sie die folgenden Schritte aus, um eine Replikationsanforderung abzulehnen, die von einem Kunden an einen externen Core gesendet wurde.

Informationen zum Ablehnen einer Anforderung, ohne sie zu überprüfen, finden Sie unter Ignorieren einer Replikationsanforderung von einem Kunden.

So lehnen Sie eine Replikationsanforderung ab

1 Öffnen Sie auf dem Ziel-Core die AppAssure Core Console und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.

2 Klicken Sie auf der Seite „Replikation“ auf **Anstehende Anforderungen (Zahl)**.

Der Abschnitt „Anstehende Replikationsanforderungen“ wird angezeigt.

3 Klicken Sie unter „Anstehende Replikationsanforderungen“ auf das Dropdown-Menü neben der Anforderung, die überprüft werden soll, und klicken Sie dann auf **Überprüfen**.

Das Fenster „Replikationsanforderung überprüfen“ wird angezeigt.

4 Klicken Sie auf **Ablehnen**.

Die Replikation wird abgelehnt. Unter „Benachrichtigungen“ auf der Registerkarte „Ereignisse“ des Quell-Core wird eine entsprechende Benachrichtigung angezeigt.

Ignorieren einer Replikationsanforderung von einem Kunden

Als externen Dienstanbieter für einen Ziel-Core können Sie eine von einem Kunden gesendete Replikationsanforderung ignorieren. Diese Möglichkeit kann genutzt werden, wenn eine Anforderung irrtümlicherweise gesendet wurde ohne eine Anforderung ohne Überprüfung abgelehnt werden soll.

Weitere Informationen zu Replikationsanforderungen finden Sie unter Überprüfen einer Replikationsanforderung von einem Kunden.

Führen Sie die folgenden Schritte aus, um eine Replikationsanforderung von einem Kunden zu ignorieren.

So ignorieren Sie eine Replikationsanforderung von einem Kunden

1 Öffnen Sie auf dem Ziel-Core die AppAssure Core Console und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.

2 Klicken Sie auf der Seite „Replikation“ auf **Anstehende Anforderungen (Zahl)**.

Der Abschnitt „Anstehende Replikationsanforderungen“ wird angezeigt.

3 Klicken Sie unter „Anstehende Replikationsanforderungen“ auf das Dropdown-Menü neben der Anforderung, die ignoriert werden soll, und klicken Sie dann auf **Ignorieren**.

4 Klicken Sie im Dialogfeld „Ignoriere Anforderung“ auf **Ja**, um den Befehl zu bestätigen.

An den Quelle-Core wird eine Benachrichtigung gesendet, dass die Anforderung ignoriert wurde, und die Anforderung wird von der Registerkarte „Replikation“ des Ziel-Core entfernt.

Hinzufügen einer Maschine zu einer bestehenden Replikation

Nachdem die Replikation zwischen einen Quell-Core und einen Ziel-Core eingerichtet wurde, besteht die Möglichkeit, neue Agenten hinzuzufügen und auf das Ziel zu replizieren. Führen Sie die folgenden Schritte aus, um einen neuen Agenten zu einem gepaarten Ziel-Core hinzuzufügen und zu replizieren.

Weitere Informationen zur Replikation finden Sie unter Informationen zur Replikation und Replikation auf einen selbstverwalteten Ziel-Core.

So fügen Sie eine Maschine zu einer bestehenden Replikation hinzu

1 Klicken Sie in der AppAssure Core Console auf die Registerkarte oder das Symbol „Replikation“.

2 Klicken Sie im Dropdown-Menü neben dem Ziel-Core, an den die neue Maschine repliziert werden soll, auf **Maschinen hinzufügen**.

Die Seite „Agenten“ des Replikationsassistenten wird geöffnet.

3 Wählen Sie auf der Seite „Agenten“ die Agenten aus, die repliziert werden sollen, und wählen Sie in den Dropdown-Listen in der Spalte „Repository“ ein Repository für jeden Agenten aus.

4 Führen Sie die folgenden Schritte aus, wenn Sie ein Seeding für die Übertragung der Basisdaten durchführen möchten:

> **HINWEIS:** Da große Datenmengen auf den Wechseldatenträger kopiert werden müssen, wird eine eSATA-, USB 3.0- oder eine andere Hochgeschwindigkeitsverbindung zum Wechseldatenträger empfohlen.

a Wählen Sie auf der Seite „Agenten“ *Seed-Laufwerk für anfängliche Übertragung verwenden* aus.

- Wenn derzeit Agenten auf einen Ziel-Core replizieren, können Sie diese Agenten in das Seed-Laufwerk einbeziehen, indem Sie **Mit bereits replizierten** auswählen.

b Klicken Sie auf **Weiter**.

c Wählen Sie auf der Seite „Seed-Laufwerkspeicherort“ in der Dropdown-Liste **Typ des Speicherorts** einen der folgenden Zieltypen aus:

- Lokal
- Netzwerk
- Cloud

d Geben Sie abhängig vom Typ des Speicherorts, der in Schritt c ausgewählt wurde, die Details für das Archiv ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 24.

Option	Textfeld	Beschreibung
Lokal	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. D:\Arbeit\Archiv.
Netzwerk	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. \\Servername\Freigabename.
	Benutzername	Geben Sie einen Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **HINWEIS:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname ist „AppAssure-5-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

e Klicken Sie auf **Weiter**.

f Geben Sie auf der Seite „Seed-Laufwerkoptionen“ die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 25.

Element	Beschreibung
Maximale Größe	Umfangreiche Datenarchive können in mehrere Segmente aufgeteilt werden. Wählen Sie den maximalen Speicherplatz aus, der zum Erstellen des Seed-Laufwerks reserviert werden soll. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie **Gesamtes Ziel** aus, um den gesamten verfügbaren Speicherplatz im Pfad, der auf der Seite „Seed-Laufwerkspeicherort“ angegeben wurde, zu reservieren. (Wenn beispielsweise „D:\Arbeit\Archiv“ als Speicherort angegeben wurde, wird der gesamte verfügbare Speicherplatz auf dem Laufwerk D: reserviert.) • Geben Sie in das leere Textfeld einen Wert ein und wählen Sie dann eine Maßeinheit in der Dropdown-Liste aus, um den maximal reservierten Speicherplatz festzulegen.
Kunden-ID (optional)	Geben Sie die Kundennummer ein, die vom Dienstanbieter zugewiesen wurde (optional).

Tabelle 25.

Element	Beschreibung
Recyclingaktion	Falls der Pfad bereits ein Seed-Laufwerk enthält, wählen Sie eine der folgenden Optionen aus: • **Nicht wiederverwenden.** Vorhandene Seed-Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, können keine Daten in das Seed-Laufwerk geschrieben werden. • **Diesen Core ersetzen.** Alle bereits vorhandenen Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert. • **Vollständig löschen.** Alle Seed-Daten werden aus dem Verzeichnis gelöscht, bevor das Seed-Laufwerk geschrieben wird.
Anmerkung	Geben Sie eine Anmerkung ein, die das Seed-Laufwerk beschreibt.
Alle Agenten zum Seed-Laufwerk hinzufügen	Wählen Sie diese Option aus, um alle Agenten im Quell-Core mit dem Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt.
Wiederherstellungspunktkette erstellen (Waisen korrigieren)	Wählen Sie diese Option aus, um die gesamte Wiederherstellungspunktkette auf das Seed-Laufwerk zu replizieren. Diese Option ist standardmäßig ausgewählt. **HINWEIS:** Beim Seeding in AppAssure 5.4 werden normalerweise nur die letzten Wiederherstellungspunkte auf das Seed-Laufwerk repliziert, um Zeitaufwand und Speicherplatz zum Erstellen des Seed-Laufwerks zu verringern. Wenn Wiederherstellungspunktketten auf dem Seed-Laufwerk erstellt werden sollen, muss auf dem Seed-Laufwerk genügend Speicherplatz zum Speichern der letzten Wiederherstellungspunkte der angegebenen Agenten vorhanden sein. Dieser Vorgang kann entsprechend länger dauern.
Kompatibles Format verwenden	Wählen Sie diese Option aus, um das Seed-Laufwerk in einem Format zu erstellen, das mit der neuen Version und älteren Versionen des AppAssure Core kompatibel ist. **HINWEIS:** Das aktuelle Seed-Laufwerksformat ist nicht kompatibel mit 5.3-Versionen des Core. Archive, die in AppAssure 5.3 erstellt wurden, sind mit AppAssure 5.4 kompatibel.

g Führen Sie eine der folgenden Aktionen aus:

- Klicken Sie auf **Weiter**, wenn das Kontrollkästchen **Alle Agenten zum Seed-Laufwerk hinzufügen** deaktiviert wurde.
- Wechseln Sie zu Schritt 5, wenn **Alle Agenten zum Seed-Laufwerk hinzufügen** aktiviert wurde.

h Wählen Sie auf der Seite „Agenten“ die Agenten aus, die mit dem Seed-Laufwerk auf den Ziel-Core repliziert werden sollen.

5 Klicken Sie auf **Finish**.

Konsumieren des Seed-Laufwerks auf einem Ziel-Core

Führen Sie die folgenden Schritte aus, um die Daten des Seed-Laufwerks auf dem Ziel-Core zu konsumieren.

HINWEIS: Diese Schritte sind nur erforderlich, wenn im Rahmen von Replikation auf einen selbstverwalteten Ziel-Core oder Replikation auf den Ziel-Core eines externen Anbieters ein Seed-Laufwerk erstellt wurde.

So konsumieren Sie das Seed-Laufwerk auf einem Ziel-Core

1 Verbinden Sie das Seed-Laufwerk mit dem Ziel-Core, wenn das Laufwerk auf einem Wechselmedium, z. B. einem USB-Laufwerk, erstellt wurde.

2 Öffnen Sie auf dem Ziel-Core die AppAssure Core Console und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.

3 Klicken Sie auf der Registerkarte „Replikation“ unter „Eingehende Replikation“ im Dropdown-Menü der zugehörigen Quell-Core auf **Konsumieren**.

Das Fenster „Konsumieren“ wird geöffnet.

4 Wählen Sie in der Dropdown-Liste **Typ des Speicherorts** eine der folgenden Optionen aus:

- Lokal
- Netzwerk
- Cloud

5 Geben Sie abhängig vom Typ des Speicherorts, der in Schritt 4 ausgewählt wurde, die Details für das Archiv ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 26.

Option	Textfeld	Beschreibung
Lokal	Speicherort	Geben Sie das Kennwort für das Archiv ein.
Netzwerk	Speicherort	Geben Sie das Kennwort für das Archiv ein.
	Benutzername	Geben Sie den Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie das Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **HINWEIS:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie den Namen des Ordners ein, in dem die archivierten Daten gespeichert sind, z. B. „AppAssure-5-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

6 Klicken Sie auf **Datei überprüfen**.

Der Core sucht nach der Datei.

Nachdem die Datei gefunden wurde, werden in die folgenden Textfelder des Fensters „Konsumieren“ die in Schritt 4, in Schritt 5 und aus der Datei erfassten Daten eingetragen. In „Datumsbereich“ werden die Datumsangaben der ältesten und neuesten Wiederherstellungspunkte im Seed-Laufwerk angezeigt. Anmerkungen, die beim Erstellen des Seed-Laufwerks eingegeben wurden, werden automatisch importiert.

7 Wählen Sie im Fenster „Konsumieren“ unter „Agenten“ die Maschinen aus, für die Daten konsumiert werden sollen.

8 Klicken Sie auf **Konsumieren**.

9 Klicken Sie auf die Registerkarte „Ereignisse“, um den Fortschritt der Datenkonsumierung zu überwachen.

Entfernen eines ausstehenden Seed-Laufwerks

Wenn Sie ein Seed-Laufwerk mit der Absicht erstellen, es auf dem Ziel-Core zu konsumieren, es aber nicht an den Remote-Standort senden, ist weiterhin ein Link für das ausstehende Seed-Laufwerk auf der Registerkarte „Replikation“ des Quell-Core vorhanden. In diesem Fall sollten Sie das ausstehende Seed-Laufwerk zugunsten anderer oder aktuellerer Daten entfernen.

Führen Sie die folgenden Schritte aus, um ein ausstehendes Seed-Laufwerk zu entfernen.

HINWEIS: Damit wird der Link zum ausstehenden Laufwerk in der AppAssure Core Console des Quell-Core entfernt. Das Laufwerk dadurch wird nicht am jeweiligen Speicherort gelöscht. Durch Entfernen des Laufwerks werden beim nächsten Replikationsjob automatisch alle Wiederherstellungspunkte des entfernten Seed-Laufwerks repliziert.

So entfernen Sie ein ausstehendes Seed-Laufwerk.

1. Öffnen Sie auf dem Quell-Core die AppAssure Core Console und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.
2. Klicken Sie auf der Seite „Replikation“ auf **Ausstehende Seed-Laufwerke (Zahl)**.

   Der Abschnitt „Ausstehende Seed-Laufwerke“ wird angezeigt. Es enthält den Namen des Remote-Ziel-Core, Datum und Uhrzeit der Erstellung des Seed-Laufwerks sowie den Datumsbereich der im Seed-Laufwerk enthaltenen Wiederherstellungspunkte.
3. Klicken Sie unter „Ausstehende Seed-Laufwerke“ auf das Dropdown-Menü neben dem Laufwerk, das entfernt werden soll, und klicken Sie dann auf **Entfernen**.

   Das Fenster „Ausstehende Seed-Laufwerke“ wird angezeigt.
4. Klicken Sie im Dialogfeld „Ausstehende Seed-Laufwerke“ zur Bestätigung auf **Ja**.

   Das Seed-Laufwerk wird entfernt.

   Wenn auf dem Quell-Core keine Seed-Laufwerke mehr vorhanden sind, werden der Link „Ausstehende Seed-Laufwerke (Zahl)“ und der Abschnitt „Ausstehende Seed-Laufwerke“ von der Registerkarte „Replikation“ entfernt.

Verwalten der Replikationseinstellungen

AppAssure bietet die Möglichkeit, die Replikation auf Gesamt-, Core- und Agentenebene zu überwachen, zu planen und anzupassen.

Sie können die folgenden Replikationseinstellungen bearbeiten:

- Informationen zum Planen von Replikationsjobs finden Sie unter Planen der Replikation.
- Informationen zum Überwachen des Fortschritts eines Replikationsjobs finden Sie unter Überwachen der Replikation.
- Informationen zum Anhalten oder Fortsetzen eines angehaltenen Replikationsjobs finden Sie unter Anhalten und Fortsetzen der Replikation.
- Informationen zum Erzwingen einer Replikation eines ein- oder ausgehenden Agenten finden Sie unter Erzwingen der Replikation.
- Informationen zum Verwalten der Einstellungen für alle Ziel-Cores und Replikationsverfahren finden Sie unter Verwalten der Einstellungen für die ausgehende Replikation.
- Informationen zum Verwalten der Einstellungen für einen bestimmten Ziel-Core finden Sie unter Ändern der Ziel-Core-Einstellungen.
- Informationen zum Verwalten der Prioritätseinstellungen für einen bestimmten Agenten, der auf einen Ziel-Core repliziert wird, finden Sie unter Festlegen der Replikationspriorität für einen Agenten.

Planen der Replikation

Sie können mit der Replikationsplanung einen Zeitpunkt, z. B. einen bestimmten Tag oder Zeiten mit geringer Auslastung, für die Übertragung replizierter Daten vom Quell-Core zum Ziel festlegen.

So planen Sie die Replikation

1. Klicken Sie in der AppAssure Core Console auf die Registerkarte oder das Symbol „Replikation“.

2 Klicken Sie auf der Registerkarte „Replikation“ auf das Dropdown-Menü neben dem Core, für den die Replikation geplant werden soll, und klicken Sie dann auf **Zeitplan**.

Das Dialogfeld „Replikationszeitplan für [Core-Name]“ wird geöffnet.

3 Wählen Sie eine der drei folgenden Optionen aus:

- **Jederzeit.** Nach jedem neuen Snapshot, nach jeder Prüfsummenprüfung und jeder Anfügbarkeitsprüfung sowie nach Abschluss der nächtlichen Jobs wird eine Replikation durchgeführt.
- **Täglich (Replikation nur im angegebenen Zeitraum starten).** Die Replikation wird nur im angegebenen Zeitraum gestartet.
    a Geben Sie im Textfeld **Von** den frühesten Zeitpunkt für den Beginn der Replikation ein.
    b Geben Sie im Textfeld **Bis** den spätesten Zeitpunkt für den Beginn der Replikation ein.

ⓘ **HINWEIS:** Wenn die Replikation am Ende der geplanten Zeit noch läuft, wird der Replikationsjob nach dem zugewiesenen Zeitraum beendet.

- **Benutzerdefiniert.** Die Replikation wird nur im angegebenen Zeitraum an den angegebenen Wochentagen durchgeführt.
    a Geben Sie neben „Wochentage“ im Textfeld **Von** den frühesten Zeitpunkt und im Textfeld **Bis** den spätesten Zeitpunkt für die Replikation an Wochentagen ein.
    b Geben Sie neben „Wochenenden“ im Textfeld **Von** den frühesten Zeitpunkt und im Textfeld **Bis** den spätesten Zeitpunkt für die Replikation an Wochenenden ein.

4 Klicken Sie auf **Speichern**.

Der Zeitplan wird für alle Replikationen zum ausgewählten Ziel-Core verwendet.

Überwachen der Replikation

Wenn die Replikation eingerichtet wurde, können Sie den Status der Replikationsaufgaben für Quell- und Ziel-Core überwachen. Sie können die Statusinformationen aktualisieren, Replikationsdetails anzeigen usw.

So überwachen Sie die Replikation

1 Klicken Sie in der Core Console auf die Registerkarte oder das Symbol „Replikation“.

2 Auf dieser Registerkarte können Sie Informationen zum Status der Replikationsaufgaben abrufen und Replikationsaufgaben überwachen (siehe Beschreibung in der folgenden Tabelle).

Tabelle 27.

Abschnitt	Beschreibung	Verfügbare Aktionen
Anstehende Replikations-anforderungen	In diesem Bereich werden Ihre Kunden-ID, E-Mail-Adresse und der Hostname aufgelistet, wenn eine Replikationsanforderung an einen externen Dienstanbieter gesendet wurde. Diese Daten werden so lange angezeigt, bis die Anforderung vom MSP akzeptiert wurde.	Klicken Sie im Dropdown-Menü auf **Ignorieren**, um die Anforderung zu ignorieren oder abzulehnen.
Ausstehende Seed-Laufwerke	In diesem Bereich werden die Seed-Laufwerke aufgelistet, die bereits geschrieben, aber noch nicht vom Ziel-Core konsumiert wurden. Angezeigt werden des Name des Remote-Core, das Erstellungsdatum und der Datumsbereich.	Klicken Sie im Dropdown-Menü auf **Entfernen**, um den Seed-Prozess zu entfernen oder abzubrechen.

Tabelle 27.

Abschnitt	Beschreibung	Verfügbare Aktionen
Ausgehende Replikation	In diesem Bereich werden alle Ziel-Cores aufgelistet, auf die der Quell-Core Daten repliziert. Angezeigt werden der Name des Remote-Core, Status, Anzahl der zu replizierenden Agent-Maschinen und der Fortschritt einer Replikationsübertragung.	Auf einem Quell-Core können Sie im Dropdown-Menü die folgenden Optionen auswählen: • **Details.** Listet ID, Anzeigename, Status, Kunden-ID, E-Mail-Adresse und Anmerkungen für den replizierten Core auf. • **Einstellungen ändern.** Listet den Anzeigenamen auf und bietet die Möglichkeit, Host und Port für den Ziel-Core zu bearbeiten. • **Löschen.** Bietet die Möglichkeit, den Ziel-Core vom Quell-Core zu löschen. Dadurch wird jegliche Replikation zu diesem Core beendet. • **Zeitplan.** Bietet die Möglichkeit, einen angepassten Zeitplan für die Replikation zum betreffenden Ziel-Core festzulegen. • **Maschinen hinzufügen.** Bietet die Möglichkeit, einen Host in einer Dropdown-Liste auszuwählen, geschützte Agenten für die Replikation auszuwählen und ein Seed-Laufwerk für die Erstübertragung des neuen Agenten zu erstellen.
Eingehende Replikation	In diesem Bereich werden alle Quellmaschinen aufgelistet, von denen das Ziel replizierte Daten empfängt. Angezeigt werden Name des Remote-Core, Status, Maschinen und Fortschritt.	Auf einem Ziel-Core können Sie im Dropdown-Menü die folgenden Optionen auswählen: • **Details.** Listet ID, Hostname, Kunden-ID, E-Mail-Adresse und Anmerkungen für den replizierten Core auf. • **Konsumieren.** Konsumiert die Anfangsdaten vom Seed-Laufwerk und speichert sie im lokalen Repository. • **Löschen.** Bietet die Möglichkeit, den Quell-Core vom Ziel-Core zu löschen. Dadurch wird jegliche Replikation von diesem Core beendet.

Anhalten und Fortsetzen der Replikation

Sie können die Replikation vorübergehend für die Quell-Cores (ausgehend) oder für die Ziel-Cores (eingehend) anhalten.

So halten Sie Replikation an und setzen Sie die Replikation fort

1. Klicken Sie in der Core Console auf die Registerkarte „Replikation“.
2. Klicken Sie auf die spitze Klammer (>), um den jeweiligen Quell- oder Ziel-Core zu erweitern.
3. Wählen Sie die Agenten aus, deren Replikation vorübergehend deaktiviert werden soll, und klicken Sie im Dropdown-Menü neben „Agent-Name“ auf **Vorübergehend deaktivieren**, um die Replikation vorübergehend anzuhalten.

   Als Status der Maschine wird „Eingerichtet (vorübergehend deaktiviert)“ in der Spalte „Status“ angezeigt.
4. Um die Replikation fortzusetzen, wählen Sie den angehaltenen Agenten aus, und klicken Sie im Dropdown-Menü „Agent-Name“ auf **Wieder aktivieren**.

Erzwingen der Replikation

Führen Sie die folgenden Schritte aus, um wie Replikation vom Quell-Core oder vom Ziel-Core aus zu erzwingen.

So erzwingen Sie eine Replikation

1. Klicken Sie in der AppAssure Core Console auf die Registerkarte oder das Symbol „Replikation“.
2. Klicken Sie auf die spitze Klammer (>), um den jeweiligen Quell- oder Ziel-Core zu erweitern.
3. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf das Dropdown-Menü neben dem Agenten, für den die Replikation erzwungen werden soll, und klicken Sie dann auf **Erzwingen**.
   - Wählen Sie die Agenten aus, deren Replikation erzwungen werden soll, und klicken Sie im Dropdown-Menü neben dem Agentennamen auf **Erzwingen**.
4. Im Dialogfeld können Sie ggf. **Verwaiste Wiederherstellungspunktketten wiederherstellen** auswählen, um verwaiste Wiederherstellungspunktketten der jeweiligen Maschine auf dem Ziel-Core zu reparieren.
5. Klicken Sie auf **Ja**.

Verwalten der Einstellungen für die ausgehende Replikation

Änderungen dieser Einstellungen wirken sich auf die Datenübertragung auf alle Ziel-Cores aus, diese diesem Quell-Core zugeordnet sind.

So verwalten Sie die Einstellungen für die ausgehende Replikation

1. Klicken Sie in der Core Console auf die Registerkarte oder das Symbol „Replikation“.
2. Klicken Sie auf **Einstellungen**.
3. Bearbeiten Sie im Fenster „Replikationseinstellungen“ die Replikationseinstellungen (siehe Beschreibung in der folgenden Tabelle).

Tabelle 28.

Option	Beschreibung
Cache-Lebensdauer (Sekunden)	Geben Sie den Zeitraum zwischen zwei Statusabfragen an den Ziel-Core durch den Quell-Core an.
Zeitüberschreitung für Volume-Image-Sitzung (Minuten)	Geben Sie den Zeitraum an, in der der Quell-Core versucht, Daten an den Ziel-Core zu übertragen.
Maximale Anzahl paralleler Streams	Geben Sie die Anzahl der zulässigen Netzwerkverbindungen an, die ein einzelner Agent für die Replikation der Daten der entsprechenden Maschine gleichzeitig verwenden darf.
Max. Übertragungsgeschwindigkeit (MB/s)	Geben Sie die maximale Geschwindigkeit für die Übertragung der replizierten Daten an.

4 Klicken Sie auf **Speichern**.

Ändern der Ziel-Core-Einstellungen

AppAssure bietet die Möglichkeit, die Host- und Porteinstellungen für einzelne Ziel-Cores zu ändern.

So ändern Sie die Ziel-Core-Einstellungen

1 Klicken Sie in der AppAssure Core Console auf die Registerkarte oder das Symbol „Replikation“.

2 Klicken Sie im Dropdown-Menü neben dem jeweiligen Ziel-Core auf **Einstellungen ändern**.

Das Fenster „Einstellungen“ wird geöffnet.

3 Bearbeiten Sie die der in der folgenden Tabelle beschriebenen Optionen.

Tabelle 29.

Option	Beschreibung
Host	Geben Sie den Host für den Ziel-Core ein.
Port	Geben Sie einen Port für die Kommunikation zwischen Ziel-Core und Quell-Core ein. HINWEIS: Die Standardportnummer ist 8006.

4 Klicken Sie auf **Speichern**.

Festlegen der Replikationspriorität für einen Agenten

Führen Sie die folgenden Schritte aus, um die Prioritätseinstellungen für die Replikation von Agent zu bearbeiten.

So legen Sie die Replikationspriorität für einen Agenten fest

1 Klicken Sie in der AppAssure Core Console auf die Registerkarte oder das Symbol „Replikation“.

2 Klicken Sie neben dem Ziel-Core auf die spitze Klammer (>), um die Replikationsagenten zu erweitern.

3 Klicken Sie auf das Dropdown-Menü für den Agenten, für den die Priorität festgelegt werden soll, und klicken Sie dann auf „Einstellungen“.

4 Wählen Sie in der Dropdown-Liste „Priorität“ eine der folgenden Optionen aus. Sie können Werte von 1 (höchste Priorität) bis 10 (geringste Priorität) auswählen. Die Standardeinstellung ist 5.

5 Klicken Sie auf **Speichern**.

Aufheben der Replikation

Sie haben mehrere Möglichkeiten, die Replikation zu deaktivieren und geschützte Maschinen aus der Replikation zu entfernen. Mögliche Optionen sind:

- Entfernen eines Agenten aus der Replikation auf dem Quell-Core
- Entfernen eines Agenten auf dem Ziel-Core
- Entfernen eines Ziel-Core aus der Replikation
- Entfernen eines Quell-Core aus der Replikation

> **HINWEIS:** Durch Entfernen eines Quell-Core werden alle replizierten Agenten entfernt, die von diesem Core geschützt werden.

Entfernen eines Agenten aus der Replikation auf dem Quell-Core

Führen Sie die folgenden Schritte aus, um einen Agenten auf dem Quell-Core aus der Replikation zu entfernen.

So entfernen Sie einen Agenten auf dem Quell-Core aus der Replikation

1. Öffnen Sie auf dem Quell-Core die AppAssure Core Console und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.
2. Erweitern Sie den Abschnitt „Ausgehende Replikation“.
3. Klicken Sie auf das Dropdown-Menü für die Agent-Maschine, die aus der Replikation entfernt werden soll, und klicken Sie dann auf **Löschen**.
4. Klicken Sie im Dialogfeld „Ausgehende Replikation“ auf **Ja**, um den Löschvorgang zu bestätigen.

Entfernen eines Agenten auf dem Ziel-Core

Führen Sie die folgenden Schritte aus, um einen Agenten auf dem Ziel-Core zu entfernen.

So entfernen Sie einen Agenten auf dem Ziel-Core

1. Öffnen Sie auf dem Ziel-Core die AppAssure Core Console und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.
2. Erweitern Sie den Abschnitt „Eingehende Replikation“.
3. Klicken Sie auf das Dropdown-Menü für die Agent-Maschine, die aus der Replikation entfernt werden soll, und klicken Sie dann auf **Löschen**.
4. Wählen Sie **mit Wiederherstellungspunkten** aus, wenn alle replizierten Wiederherstellungspunkte, die von der betreffenden Maschine empfangen wurden, zusammen mit dem Agenten gelöscht werden sollen.
5. Klicken Sie im Dialogfeld „Eingehende Replikation“ auf **Ja**, um den Löschvorgang zu bestätigen.

Entfernen eines Ziel-Core aus der Replikation

Führen Sie die nachstehend beschriebenen Schritte aus, um einen Ziel-Core aus der Replikation zu entfernen.

So entfernen Sie einen Ziel-Core aus der Replikation

1. Öffnen Sie auf dem Quell-Core die AppAssure Core Console und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.

2 Klicken Sie unter „Ausgehende Replikation“ auf das Dropdown-Menü neben dem Remote-Core, der gelöscht werden soll, und klicken Sie auf **Löschen**.

3 Klicken Sie im Dialogfeld „Ausgehende Replikation“ auf **Ja**, um den Löschvorgang zu bestätigen.

Entfernen eines Quell-Core aus der Replikation

Führen Sie die nachstehend beschriebenen Schritte aus, um einen Quell-Core aus der Replikation zu entfernen.

HINWEIS: Durch Entfernen eines Quell-Core werden alle replizierten Agenten entfernt, die von diesem Core geschützt werden.

So entfernen Sie einen Quell-Core aus der Replikation

1 Öffnen Sie auf dem Ziel-Core die AppAssure Core Console und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.

2 Klicken Sie unter „Eingehende Replikation“ im Dropdown-Menü auf **Löschen**.

3 Wählen Sie **mit Wiederherstellungspunkten** aus, wenn alle replizierten Wiederherstellungspunkte, die von der betreffenden Maschine empfangen wurden, zusammen mit dem Quell-Core gelöscht werden sollen.

4 Klicken Sie im Dialogfeld „Eingehende Replikation“ auf **Ja**, um den Löschvorgang zu bestätigen.

Wiederherstellen von replizierten Daten

Die alltägliche Replikationsfunktion wird auf dem Quell-Core verwaltet. Auf dem Ziel-Core können nur die für eine Notfallwiederherstellung notwendigen Funktionen durchgeführt werden.

Für eine Notfallwiederherstellung kann der Ziel-Core die replizierten Wiederherstellungspunkte verwenden, um die geschützten Agenten und den Core wiederherzustellen. Sie können die folgenden Wiederherstellungsoptionen auf dem Ziel-Core durchführen:

- Wiederherstellungspunkte bereitstellen. Weitere Informationen finden Sie unter Bereitstellen eines Wiederherstellungspunktes für eine Windows-Maschine.
- Rollback auf Wiederherstellungspunkte durchführen. Weitere Informationen finden Sie unter Wiederherstellen von Volumes aus einem Wiederherstellungspunkt bzw. Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile.
- Export einer virtuellen Maschine (VM) durchführen. Weitere Informationen finden Sie unter Exportieren von Daten aus einer Windows-Maschine in eine virtuelle Maschine.
- BMR-Wiederherstellung (Bare Metal Restore) durchführen. Weitere Informationen finden Sie unter Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen.
- Failback durchführen (falls eine Failover/Failback-Replikationsumgebung eingerichtet wurde). Weitere Informationen finden Sie unter Durchführen eines Failbacks.

Anleitung für Failover und Failback

Wenn Sie mit einer Notfallsituation konfrontiert sind, in der der Quell-Core und der zugehörige Agent ausgefallen sind, können Sie in AppAssure einen Failover aktivieren, um den Schutz auf einen identischen Failover-Core (Ziel-Core) zu verlagern und einen neuen (replizierten) Agenten zu starten, der mit dem ausgefallen Agenten identisch ist. Nachdem der Quell-Core und die Agenten repariert wurden, können Sie ein Failback durchführen, um die Daten von Failover-Core und -Agent auf dem Quell-Core und -Agent wiederherzustellen. In AppAssure umfassen Failover und Failback die folgenden Verfahren.

- **Einrichten der Umgebung für ein Failover.** Siehe Abschnitt Einrichten einer Umgebung für Failover.

- **Durchführen eines Failovers für den Ziel-Core und die zugehörigen Agenten.** Siehe Abschnitt Durchführen eines Failovers auf dem Ziel-Core.
- **Wiederherstellen eines Quell-Core durch Durchführen eines Failbacks.** Siehe Abschnitt Durchführen eines Failovers auf dem Ziel-Core.

Einrichten einer Umgebung für Failover

Beim Einrichten Ihrer Umgebung für Failover müssen ein AppAssure Quell- und Ziel-Core sowie der zugehörige Agent für die Replikation eingerichtet werden. Führen Sie die folgenden Schritte durch, um eine Replikation für Failover einzurichten.

So richten Sie eine Umgebung für ein Failover ein

1. Installieren Sie einen AppAssure Core für die Quelle und einen AppAssure Core für das Ziel. Weitere Informationen finden Sie im *Dell AppAssure Bereitstellungshandbuch*.
2. Installieren Sie einen AppAssure Agent, der durch den Quell-Core geschützt wird. Weitere Informationen finden Sie im *Dell AppAssure Bereitstellungshandbuch*.
3. Erstellen Sie ein Repository im Quell-Core und ein Repository im Ziel-Core. Weitere Informationen finden Sie unter Erstellen eines Repositorys.
4. Fügen Sie den zu schützenden Agenten zum Quell-Core hinzu. Weitere Informationen finden Sie unter Schützen einer Maschine.
5. Richten Sie Replikation vom Quell- auf den Ziel-Core ein und replizieren Sie den geschützten Agenten mit allen Wiederherstellungspunkten. Folgen Sie dazu den Anweisungen im Abschnitt Replikation auf einen selbstverwalteten Ziel-Core, um den Ziel-Core hinzuzufügen, auf den die Replikation erfolgen soll.

Durchführen eines Failovers auf dem Ziel-Core

Wenn Sie mit einer Notfallsituation konfrontiert sind, in der der Quell-Core und die zugehörigen Agenten ausgefallen sind, können Sie in AppAssure einen Failover aktivieren, um den Schutz auf einen identischen Failover-Core (Ziel-Core) zu verlagern. Der Ziel-Core ist dann der einzige Core, der die Daten in der Umgebung schützt. Starten Sie dann einen neuen Agenten, der den ausgefallenen Agenten vorübergehend ersetzt.

So führen Sie ein Failover auf dem Ziel-Core durch

1. Navigieren Sie zur AppAssure Core Console auf dem Ziel-Core und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.
2. Erweitern Sie unter „Eingehende Replikation“ die Details des ausgewählten Quell-Core.
3. Wählen Sie im Dropdown-Menü des gewünschten Agenten auf **Failover** aus.

   Im Dialogfeld „Failover“ werden die nächsten erforderlichen Schritte für einen Failover angezeigt.

   - Wählen Sie **Replikationsjob abbrechen (sofern aktiv)** aus, um alle aktiven Replikationsjobs für den Agenten zu beenden.
4. Klicken Sie auf **Weiter**.
5. Wählen Sie im linken Navigationsbereich unter „Geschützte Maschinen“ die Maschine aus, auf dem sich der entsprechende AppAssure Agent mit den Wiederherstellungspunkten befindet.
6. Exportieren Sie die Sicherungsinformationen zum Wiederherstellungspunkt auf dem Agenten in eine virtuelle Maschine. Weitere Informationen finden Sie unter Exportieren von Daten aus einer Windows-Maschine in eine virtuelle Maschine.
7. Starten Sie die virtuelle Maschine, auf der sich nun die exportierten Sicherungsinformationen befinden. Warten Sie, bis die Gerätetreibersoftware installiert wurde.
8. Starten Sie die virtuelle Maschine neu und warten Sie, dass der Agent-Dienst gestartet wird.

9 Wechseln Sie wieder zur AppAssure Core Console für den Ziel-Core und überprüfen Sie, ob der neue Agent im linken Navigationsbereich unter „Geschützte Maschinen“ und auf der Registerkarte „Replikation“ unter „Eingehende Replikation“ angezeigt wird.

10 Erzwingen Sie mehrere Snapshots und überprüfen Sie, ob diese ordnungsgemäß durchgeführt wurden. Weitere Informationen finden Sie unter Erzwingen eines Snapshots.

11 Sie können nun ein Failback durchführen. Entsprechende Informationen finden Sie im folgenden Abschnitt Durchführen eines Failbacks.

Durchführen eines Failbacks

Nachdem Sie den fehlerhaften Ursprungsquell-Core und die Agenten repariert oder ersetzt haben, müssen Sie die Daten von den Failover-Maschinen verschieben, um die Quellmaschinen wiederherzustellen.

So führen Sie ein Failback aus

1 Navigieren Sie zur AppAssure Core Console auf dem Ziel-Core und klicken Sie auf die Registerkarte oder das Symbol „Replikation“.

2 Wählen Sie unter „Eingehende Replikation“ den Failover-Agenten aus und erweitern Sie die Details.

3 Klicken Sie im Menü „Aktionen“ auf **Failback**.

Im Dialogfeld „Failback“ werden die erforderlichen Schritte aufgelistet werden, die durchgeführt werden müssen, bevor Sie auf „Weiter“ klicken, um den Failback durchzuführen.

4 Klicken Sie auf **Abbrechen**.

5 Wenn auf der Failover-Maschine Microsoft SQL Server oder Microsoft Exchange Server ausgeführt wird, beenden Sie diese Dienste.

6 Erzwingen Sie einen Snapshot der Maschine. Weitere Informationen finden Sie unter Erzwingen eines Snapshots.

7 Fahren Sie die Failover-Maschine herunter.

8 Erstellen Sie ein Archiv auf dem Failover-Agenten und speichern Sie es auf einem Datenträger oder einem freigegebenen Netzwerkspeicherort. Weitere Informationen dazu finden Sie unter Erstellen eines Archivs.

9 Navigieren Sie nach dem Erstellen des Archivs zur AppAssure Core Console im neu reparierten Quell-Core und klicken Sie auf die Registerkarte „Extras“.

10 Importieren Sie das Archiv, das Sie soeben in Schritt 8 erstellt haben. Weitere Informationen dazu finden Sie unter Importieren eines Archivs.

11 Wechseln Sie wieder zur Core Console auf dem Ziel-Core und klicken Sie auf die Registerkarte „Replikation“.

12 Wählen Sie unter „Eingehende Replikation“ den Failover-Agenten aus und erweitern Sie die Details.

13 Wählen Sie im Dropdown-Menü des Agenten auf **Failback** aus.

14 Klicken Sie im Dialogfeld „Failback“ auf **Weiter**.

15 Fahren Sie die Maschine herunter, die den exportierten Agenten enthält, der beim Failover erstellt wurde.

16 Führen Sie eine BMR-Wiederherstellung (Bare Metal Restore) für den Quell-Core und -Agent durch. Weitere Informationen finden Sie unter Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen.

> **HINWEIS:** Wenn Sie die Wiederherstellung starten (siehe Beschreibung in Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung), müssen Sie die Wiederherstellungspunkte verwenden, die vom Ziel-Core in den Agenten der virtuellen Maschine importiert wurden.

17 Warten Sie, bis der BMR-Neustart durchgeführt und der Agent-Dienst gestartet wurde. Zeigen Sie die Details der Netzwerkverbindung der Maschine an und notieren Sie diese.

18 Navigieren Sie in der Core Console auf dem Quell-Core zur entsprechenden Maschine und ändern Sie die Maschinenschutzeinstellungen, um die neuen Netzwerkverbindungsdetails hinzuzufügen. Weitere Informationen finden Sie unter Konfigurieren von Maschineneinstellungen.

19 Navigieren Sie zur Core Console auf dem Ziel-Core und löschen Sie dort den Agenten aus der Registerkarte „Replikation“. Weitere Informationen finden Sie unter Aufheben der Replikation.

20 Richten Sie in der Core Console des Quell-Core wieder die Replikation zwischen Quelle und Ziel ein. Klicken Sie dazu auf die Registerkarte „Replikation“ und fügen Sie den Ziel-Core für die Replikation hinzu. Weitere Informationen dazu finden Sie unter Replikation auf einen selbstverwalteten Ziel-Core.Aufheben der Replikation.

Verwalten von Ereignissen

Durch die Verwaltung von Core-Ereignissen wird die Überwachung des Funktionszustands und der Nutzung des AppAssure Core erleichtert. Der Core umfasst vordefinierte Ereignisse, mit denen Administratoren über kritische Probleme im Core oder in Sicherungsjobs benachrichtigt werden können.

Im Abschnitt „Ereignisse“ des Abschnitts „Konfiguration“ der Registerkarte „Konfiguration“ können Sie Benachrichtigungsgruppen, E-Mail-SMTP-Einstellungen, Reduzierung von Wiederholungen und Ereignisaufbewahrung verwalten. Die Option „Benachrichtigungsgruppen“ in AppAssure ermöglicht die Verwaltung von Benachrichtigungsgruppen. Diese bieten folgende Möglichkeiten:

- Festlegen eines Ereignisses, für das eine Benachrichtigung generiert werden soll.
- Festlegen der Art der Benachrichtigung.
- Festlegen der Empfänger und des Absenders der Benachrichtigung. Mögliche Optionen sind.
- Festlegen einer Zeitgrenze für Wiederholungen.
- Festlegen des Aufbewahrungszeitraums für alle Ereignisse.

Konfigurieren von Benachrichtigungsgruppen

Führen Sie die folgenden Schritte aus, um Benachrichtigungsgruppen für Benachrichtigungen zu konfigurieren.

HINWEIS: Sie müssen darüber hinaus SMTP-Servereinstellungen (Simple Mail Transfer Protocol) konfigurieren, wenn Benachrichtigungen als E-Mail-Nachrichten gesendet werden sollen (siehe nachstehende Beschreibung). Weitere Informationen zum Festlegen von Konfigurationseinstellungen für SMTP-Server finden Sie unter Konfigurieren eines E-Mail-Servers.

So konfigurieren Sie Benachrichtigungsgruppen

1 Navigieren Sie zum AppAssure Core, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Ereignisse**.

2 Klicken Sie auf **Gruppe hinzufügen**.

Das Dialogfeld „Benachrichtigungsgruppe hinzufügen“ wird angezeigt.

Das Dialogfeld „Benachrichtigungsgruppe hinzufügen“ enthält einen allgemeinen Beschreibungsbereich und zwei Registerkarten:

- Benachrichtigungen aktivieren
- Benachrichtigungsoptionen

3 Geben Sie die in der folgenden Tabelle beschriebenen grundlegenden Informationen für die Benachrichtigungsgruppe ein.

Tabelle 30.

Textfeld	Beschreibung
Name	Geben Sie einen Namen für die Ereignisbenachrichtigungsgruppe ein. Er wird zur Identifizierung der Ereignisbenachrichtigungsgruppe verwendet. Diese Information ist erforderlich.
Beschreibung	Geben Sie eine Beschreibung für die Ereignisbenachrichtigungsgruppe ein. Sie wird zur Beschreibung des Zwecks der Ereignisbenachrichtigungsgruppe verwendet. Diese Information ist optional.

4 Legen Sie auf der Registerkarte „Benachrichtigungen aktivieren“ wie folgt die Systemereignisse fest, die protokolliert, für die Berichte erstellt und über die Sie benachrichtigt werden sollen:

- Wählen Sie **Alle Benachrichtigungen** aus, wenn für alle Ereignisse Benachrichtigungen erstellt werden sollen.
- Wenn Benachrichtigungen für Fehler, Warnungen oder informative Meldungen erstellt werden sollen, wählen Sie neben „Typen auswählen“ die entsprechende Option aus:
  - Fehler (rotes Dreieckssymbol)
  - Warnung (gelbes Dreieckssymbol)
  - Info (blauer Kreis)
  - Standardeinstellungen wiederherstellen (gekrümmter Pfeil)
- Gehen Sie folgendermaßen vor, um Benachrichtigungen für bestimmte Ereignisse zu erstellen:
  a Klicken Sie auf die spitze Klammer (>) neben „Alle Benachrichtigungen“, um die Ansicht zu erweitern und die Ereignisse, für die Benachrichtigungen festgelegt werden können, nach Gruppen geordnet anzuzeigen. Die Kategorien für Ereignisgruppen umfassen:
    - Alle Ereignisse
    - Exchange
    - Autom. Aktualisierung
    - Deduplizierungscache
    - Wiederherstellungspunkt-Prüfung
    - Remote-Bereitstellung
    - Start-CD
    - Sicherheit
    - Datenbankaufbewahrung
    - Lokale Bereitstellung
    - Metadaten
    - Cluster
    - Benachrichtigung
    - PowerShell Scripting
    - Push-Installation
    - Anfügbarkeit
    - Jobs
    - Lizenzierung
    - Protokollkürzung
    - Archiv

- Core-Dienst
- Export
- Schutz
- Replikation
- Repository
- Rollback (Wiederherstellung)
- Rollup

b Klicken Sie zum Anzeigen der einzelnen Ereignisse in einer Gruppe auf die rechte spitze Klammer (>) neben der jeweiligen Gruppe und wählen Sie dann die Ereignisse aus, für die Protokolleinträge erstellt, Berichte erstellt und Benachrichtigungen festgelegt werden sollen.

c Um Benachrichtigungen für alle Ereignisse in einer Gruppe zu erstellen, aktivieren Sie das Kontrollkästchen neben der betreffenden Gruppe.

5 Klicken Sie auf die Registerkarte „Benachrichtigungsoptionen“.

6 Geben Sie auf der Registerkarte „Benachrichtigungsoptionen“ an, wie die Benachrichtigung erfolgen soll.

In der folgenden Tabelle werden die Benachrichtigungsoptionen beschrieben.

Tabelle 31.

Textfeld	Beschreibung
Per E-Mail benachrichtigen	Geben Sie die Empfänger der E-Mail-Benachrichtigung an. Sie können entweder mehrere getrennte E-Mail-Adressen sowie BCC- und CC-Empfänger angeben. Folgende Optionen stehen zur Auswahl: • An: • CC: • BCC:
Über Windows-Ereignisprotokoll benachrichtigen	Wählen Sie diese Option, wenn Benachrichtigungen über das Windows-Ereignisprotokoll gemeldet werden sollen.
Über syslogd benachrichtigen	Wählen Sie diese Option, wenn Benachrichtigungen durch syslogd gemeldet werden sollen. Geben Sie die Details für syslogd in den folgenden Textfeldern an: • Host: • Port:
Über Popupbenachrichtigungen benachrichtigen	Wählen Sie diese Option aus, wenn die Benachrichtigung als Popup in der unteren rechten Ecke des Bildschirms angezeigt werden soll.

7 Klicken Sie auf **OK**.

Es wird eine Meldung mit dem Hinweis angezeigt, dass der festgelegte Name der Benachrichtigungsgruppe nicht mehr geändert werden kann, nachdem die Gruppe erstellt wurde. Die anderen Eigenschaften der Benachrichtigungsgruppe können jederzeit geändert werden.

- Bestätigen Sie die Meldung, wenn Sie den eingegebenen Gruppennamen verwenden möchten, um die Einstellungen zu speichern.
- Klicken Sie auf **Nein**, wenn Sie den Gruppennamen ändern möchten, um zum Fenster zum Erstellen der Benachrichtigungsgruppe zurückzukehren. Aktualisieren Sie dort den Gruppenname und ggf. andere Einstellungen für die Benachrichtigungsgruppe und speichern Sie die Einstellungen.

Konfigurieren eines E-Mail-Servers

Führen Sie die folgenden Schritte aus, um einen E-Mail-Server zu konfigurieren.

HINWEIS: Darüber hinaus müssen Sie Einstellungen für Benachrichtigungsgruppen konfigurieren, z. B. die Option „Per E-Mail benachrichtigen“ aktivieren, damit E-Mail-Benachrichtigungen gesendet werden können. Weitere Informationen zum Angeben von Ereignissen, für die E-Mail-Benachrichtigungen erstellt werden sollen, finden Sie unter Konfigurieren von Benachrichtigungsgruppen.

So konfigurieren Sie einen E-Mail-Server

1 Navigieren Sie zum AppAssure Core, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Ereignisse**.

2 Klicken Sie im Bereich „E-Mail-Einstellungen“ auf **SMTP-Server**.

Das Dialogfeld „SMTP-Servereinstellungen“ wird angezeigt.

3 Geben Sie die Details für den E-Mail-Server ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 32.

Textfeld	Beschreibung
SMTP-Server	Geben Sie den Namen des E-Mail-Servers an, der von der E-Mail-Benachrichtigungsvorlage verwendet werden soll. Angegeben werden müssen Hostname, Domäne und Suffix, z.B. smtp.gmail.com.
Von	Geben Sie eine Absender-E-Mail-Adresse ein. Diese Option wird zur Angabe der Absender-E-Mail-Adresse für die E-Mail-Benachrichtigungsvorlage verwendet, z. B. noreply@localhost.com.
Benutzername	Geben Sie einen Benutzernamen für den E-Mail-Server ein.
Kennwort	Geben Sie das erforderliche Kennwort für den Benutzernamen für den Zugriff auf den E-Mail-Server ein.
Port	Geben Sie eine Portnummer ein. Sie wird zur Angabe des Ports für den E-Mail-Server verwendet, z. B. Port 587 für Gmail. Die Standardeinstellung ist *25*.
Zeitüberschreitung (Sekunden)	Geben Sie einen ganzzahligen Wert für den Zeitraum ein, in dem eine Verbindung zum E-Mail-Server hergestellt werden soll. Der Zeitraum vor einer Zeitüberschreitung wird in Sekunden angegeben. Die Standardeinstellung ist *60 Sekunden*.
TLS	Wählen Sie diese Option aus, wenn der E-Mail-Server eine sichere Verbindung verwendet, z. B. Transport Layer Security (TLS) oder Secure Sockets Layer (SSL).

4 Klicken Sie auf **Test-E-Mail senden** und führen Sie die folgenden Aktionen aus:

a Geben Sie im Dialogfeld „Test-E-Mail senden“ eine E-Mail-Zieladresse für die Testnachricht ein und klicken Sie auf **Senden**.

b Schließen Sie das Fehlerdialogfeld und das Dialogfeld „Test-E-Mail senden“, wenn die Testnachricht fehlschlägt, und ändern Sie die Konfigurationseinstellungen für den E-Mail-Server. Wiederholen Sie anschließend Schritt 4.

c Klicken Sie auf **OK**, wenn die Testnachricht erfolgreich gesendet wurde, um dies zu bestätigen.

d Überprüfen Sie das E-Mail-Konto, an das die Test-E-Mail-Nachricht gesendet wurde.

e Kehren Sie wieder zum Dialogfeld „SMTP-Servereinstellungen“ zurück, wenn Sie mit den Testergebnissen zufrieden sind, und klicken Sie auf **Speichern**, um das Dialogfeld zu schließen und die Änderungen zu speichern.

Konfigurieren einer E-Mail-Benachrichtigungsvorlage

Führen Sie die folgenden Schritte aus, um eine E-Mail-Benachrichtigungsvorlage zu konfigurieren. Diese Vorlage wird vom SMTP-E-Mail-Server zum Senden von Benachrichtigungen für AppAssure-Ereignisse per E-Mail verwendet.

HINWEIS: Darüber hinaus müssen Sie einen E-Mail-Server und Einstellungen für Benachrichtigungsgruppen konfigurieren, z. B. die Option **Per E-Mail benachrichtigen** aktivieren, damit E-Mail-Benachrichtigungen gesendet werden können. Weitere Informationen zum Konfigurieren eines E-Mail-Servers zum Senden von Benachrichtigungen finden Sie unter Konfigurieren eines E-Mail-Servers. Weitere Informationen zum Angeben von Ereignissen, für die E-Mail-Benachrichtigungen erstellt werden sollen, finden Sie unter Konfigurieren von Benachrichtigungsgruppen.

So konfigurieren Sie eine E-Mail-Benachrichtigungsvorlage

1. Navigieren Sie zum AppAssure Core, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Ereignisse**.
2. Klicken Sie im Bereich „E-Mail-Einstellungen“ auf **Ändern**.

   Das Dialogfeld „Konfiguration der E-Mail-Benachrichtigung bearbeiten“ wird angezeigt.
3. Wählen Sie **E-Mail-Benachrichtigungen aktivieren** aus.
4. Geben Sie in das Textfeld „E-Mail-Betreff“ einen Betreff für die E-Mail-Vorlage ein.

   Der E-Mail-Betreff wird zur Definition des Betreffs der E-Mail-Benachrichtigungsvorlage verwendet, z. B. <Hostname> - <Stufe> <Name>.
5. Geben Sie im Textfeld „E-Mail“ die Informationen für den Nachrichtentext der Benachrichtigung ein, der das Ereignis, den Zeitpunkt, zu dem das Ereignis aufgetreten ist, und den Schweregrad beschreibt.
6. Klicken Sie auf **Test-E-Mail senden** und führen Sie die folgenden Aktionen aus:
   a. Geben Sie im Dialogfeld „Test-E-Mail senden“ eine E-Mail-Zieladresse für die Testnachricht ein und klicken Sie auf **Senden**.
   b. Schließen Sie das Fehlerdialogfeld und das Dialogfeld „Test-E-Mail senden“, wenn die Testnachricht fehlschlägt. Klicken Sie auf **OK**, um die aktuellen Einstellungen für die E-Mail-Vorlage zu speichern, und ändern Sie die E-Mail-Servereinstellungen (siehe Beschreibung in Konfigurieren eines E-Mail-Servers). Achten Sie darauf, dass Sie das Kennwort für das E-Mail-Konto erneut eingeben. Speichern Sie die Einstellungen und kehren Sie hierher zurück.
   c. Klicken Sie auf **OK**, wenn die Testnachricht erfolgreich gesendet wurde, um dies zu bestätigen.
   d. Überprüfen Sie das E-Mail-Konto, an das die Test-E-Mail-Nachricht gesendet wurde.
   e. Kehren Sie wieder zum Dialogfeld „Konfiguration der E-Mail-Benachrichtigung bearbeiten“ zurück, wenn Sie mit den Testergebnissen zufrieden sind, und klicken Sie auf **Speichern**, um das Dialogfeld zu schließen und die Änderungen zu speichern.

Konfigurieren der Reduzierung der Wiederholungen

Führen Sie die folgenden Schritte aus, um die Reduzierung der Wiederholungen für Ereignisse zu konfigurieren.

So konfigurieren Sie die Reduzierung der Wiederholungen

1. Klicken Sie auf der AppAssure Core-Startseite im Dropdown-Menü „Konfiguration“ auf **Ereignisse**.
2. Klicken Sie im Bereich „Reduzierung der Wiederholungen“ auf **Ändern**.

   Das Dialogfeld „Reduzierung der Wiederholungen“ wird angezeigt.
3. Wählen Sie **Reduzierung der Wiederholungen aktivieren** aus.
4. Geben Sie im Textfeld **Ereignisse speichern für** mit dem Aufwärts- und Abwärtspfeil den Zeitraum in Minuten ein, für den Ereignisse gespeichert werden sollen, um Wiederholungen zu reduzieren.
5. Klicken Sie auf **OK**.

Konfigurieren der Ereignisaufbewahrung

Führen Sie die folgenden Schritte aus, um die Aufbewahrung von Ereignissen zu konfigurieren.

So konfigurieren Sie die Ereignisaufbewahrung

1. Klicken Sie auf der AppAssure Core-Startseite im Dropdown-Menü „Konfiguration“ auf **Einstellungen**.
2. Klicken Sie unter „Einstellungen für Datenbankverbindung“ auf **Ändern**.

   Das Dialogfeld „Datenbankverbindungseinstellungen“ wird angezeigt.
3. Geben Sie im Textfeld **Ereignis- und Jobverlauf beibehalten für (Dauer)** die Anzahl der Tage ein, für die Informationen für Ereignisse aufbewahrt werden sollen, z. B. *30 Tage* (Standardeinstellung).
4. Klicken Sie auf **Speichern**.

Verwalten der Wiederherstellung

Der AppAssure Core kann Daten sofort wiederherstellen oder ausgehend von den Wiederherstellungspunkten Maschinen in physische oder virtuelle Maschinen wiederherstellen. Die Wiederherstellungspunkte enthalten Snapshots der Agenten-Volumes, die auf Blockebene erfasst werden. Diese Snapshots sind anwendungskonsistent, d. h. dass alle offenen Transaktionen und laufenden Transaktionsprotokolle abgeschlossen und die Cache-Speicher auf der Festplatte abgelegt werden, bevor der Snapshot erstellt wird. Bei Verwendung anwendungskonsistenter Snapshots zusammen mit Verified Recovery kann der Core verschiedenartige Wiederherstellungen durchführen, z. B.:

- Wiederherstellung von Dateien und Ordnern
- Wiederherstellung von Daten-Volumes mithilfe von Live Recovery
- Wiederherstellung von Daten-Volumes für Microsoft Exchange Server und Microsoft SQL Server mithilfe von Live Recovery
- Bare Metal Restore mithilfe von Universal Recovery
- BMR-Wiederherstellung (Bare Metal Restore) auf anderer Hardware mithilfe von Universal Recovery
- Ad-hoc- und fortlaufender Export in virtuelle Maschinen

Informationen zu Systeminformationen

AppAssure bietet die Möglichkeit, Informationen zum AppAssure Core anzuzeigen, z. B. Systeminformationen, lokale und bereitgestellte Volumes sowie AppAssure Engine-Verbindungen.

Wenn Sie die Bereitstellung einzelner oder aller Wiederherstellungspunkte, die lokal auf einem Core bereitgestellt wurden, aufheben möchten, können Sie dies über die Option „Bereitstellung“ auf der Registerkarte „Extras“ erledigen. Weitere Informationen zum Aufheben der Bereitstellung von Wiederherstellungspunkten finden Sie unter Aufheben der Bereitstellung ausgewählter Wiederherstellungspunkte und Aufheben der Bereitstellung aller Wiederherstellungspunkte.

Anzeigen von Systeminformationen

Führen Sie die folgenden Schritte aus, um Systeminformationen anzuzeigen.

So zeigen Sie Systeminformationen an

1. Navigieren Sie zum AppAssure Core und wählen Sie die Registerkarte „Extras“ aus.
2. Klicken Sie unter „Extras“ auf **Systeminformationen**.

Herunterladen von Installationsprogrammen

AppAssure bietet die Möglichkeit, Installationsprogramme vom AppAssure Core herunterzuladen. Auf der Registerkarte „Extras“ können Sie den Agent Installer oder das Local Mount Utility herunterladen.

HINWEIS: Informationen zum Zugriff auf den Agent Installer finden Sie unter Herunterladen des Agent Installers. Weitere Informationen zum Bereitstellen des Agent Installers finden Sie im *Dell AppAssure Bereitstellungshandbuch*. Informationen zum Zugriff auf das Installationsprogramm für das Local Mount Utility finden Sie unter Informationen zum Local Mount Utility Weitere Informationen zum Local Mount Utility finden Sie unter So laden Sie das Local Mount Utility herunter und installieren Sie es.

Informationen zum Agent Installer

Der Agent Installer wird verwendet, um die AppAssure Agent-Anwendung auf Maschinen zu installieren, die durch den AppAssure Core geschützt werden sollen. Wenn Sie feststellen, dass der Agent Installer auf einer Maschine installiert werden muss, können Sie das Webinstallationsprogramm über die Registerkarte „Extras“ des AppAssure Core herunterladen.

HINWEIS: Der Core wird vom Dell Software-Lizenzportal heruntergeladen. Weitere Informationen zum Herunterladen des AppAssure Core Installers finden Sie unter „https://licenseportal.com“.

Herunterladen des Agent Installers

Sie können den AppAssure Agent Installer herunterladen und auf jeder Maschine installieren, die durch den AppAssure Core geschützt wird. Führen Sie die folgenden Schritte aus, um das Webinstallationsprogramm herunterzuladen.

AppAssureSo laden Sie den Agent Installer herunter

1. Laden Sie den AppAssure Agent Installer vom Dell Software-Lizenzportal oder dem AppAssure Core herunter. Beispiel:

   ```
   Agent-X64-5.2.1.xxxxx.exe
   ```

2. Klicken Sie auf **Datei speichern**.

   Weitere Informationen zum Installieren von Agenten finden Sie im *Dell AppAssure Bereitstellungshandbuch*.

Informationen zum Local Mount Utility

Das Local Mount Utility ist eine herunterladbare Anwendung, mit der Sie einen Wiederherstellungspunkt in einem remote AppAssure Core auf einer beliebigen Maschine bereitstellen können. Das kompakte Dienstprogramm umfasst die Treiber *aavdisk* und *aavstor*, wird aber nicht als Dienst ausgeführt. Wenn Sie das Programm installieren, wird es standardmäßig im Verzeichnis C:\Program Files\AppRecovery\Local Mount Utility installiert und es wird eine Verknüpfung auf dem Desktop der Maschine erstellt.

Das Local Mount Utility wurde zwar für den Remote-Zugriff auf Cores konzipiert. Sie können das Programm aber auch in einem AppAssure Core installieren. Wenn es in einem Core ausgeführt wird, erkennt es alle Bereitstellungen dieses Core und zeigt sie an, einschließlich der Bereitstellungen durch die AppAssure Core Console. Genauso werden auch Bereitstellungen, die durch das Local Mount Utility durchgeführt wurden, in der Konsole angezeigt.

So laden Sie das Local Mount Utility herunter und installieren Sie es

In AppAssure können Sie das Local Mount Utility direkt in der AppAssure Core Console herunterladen. Führen Sie die folgenden Schritte durch, um das Programm herunterzuladen und zu installieren.

So laden Sie das Local Mount Utility herunter und installieren Sie es

1. Öffnen Sie auf der Maschine, auf der Sie das Local Mount Utility installieren möchten, die AppAssure Core Console. Geben Sie dazu die Konsolen-URL im Browser ein und melden sich mit Ihrem Benutzernamen und Kennwort an.
2. Wählen Sie in der AppAssure Core Console die Registerkarte „Extras“ aus.
3. Klicken Sie auf der Registerkarte „Extras“ auf **Downloads**.
4. Klicken Sie unter „Local Mount Utility“ auf den Link **Webinstallationsprogramm herunterladen**.
5. Klicken Sie im Fenster „LocalMountUtility-Web.exe wird geöffnet“ auf **Datei speichern**.

   Die Datei wird im lokalen Ordner „Downloads“ gespeichert. In manchen Browsern wird der Ordner automatisch geöffnet.
6. Klicken Sie im Ordner „Downloads“ mit der rechten Maustaste auf die Datei LocalMountUtility-Web.exe und klicken Sie auf **Öffnen**.

   Je nach Konfiguration der Maschine wird u. U. das Fenster „Benutzerkontensteuerung“ angezeigt.
7. Klicken Sie im Fenster „Benutzerkontensteuerung“ auf **Ja**, damit das Programm Änderungen an der Maschine vornehmen kann.

   Der Installationsassistent für das AppAssure Local Mount Utility wird gestartet.
8. Klicken Sie in der Begrüßungsanzeige des Installationsassistenten für das AppAssure Local Mount Utility auf **Weiter**, um zur Seite „Lizenzvereinbarung“ zu gelangen.
9. Wählen Sie auf der Seite „Lizenzvereinbarung“ die Option **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus, und klicken Sie dann auf **Weiter**, um zur Seite „Erforderliche Komponenten“ zu gelangen.
10. Installieren Sie auf der Seite „Erforderliche Komponenten“ alle erforderlichen Komponenten und klicken Sie auf **Weiter**, um zur Seite „Installationsoptionen“ zu gelangen.
11. Führen Sie auf der Seite „Installationsoptionen“ die folgenden Aufgaben durch:
    a. Wählen Sie einen Zielordner für das Local Mount Utility aus, indem Sie auf die Schaltfläche **Ändern** klicken.

       HINWEIS: Der Standardzielordner ist „C:\Program Files\AppRecovery\LocalMountUtility“.

    b. Wählen Sie ggf. die Option **Local Mount Utility berechtigen, Diagnose- und Auslastungsdaten automatisch an AppAssure Software, Inc. zu senden** aus.

    c. Wählen Sie **Optional Komponenten auswählen: Mailbox Restore** aus.

    d. Klicken Sie auf **Weiter**, um zur Seite „Fortschritt“ zu gelangen und die Anwendung herunterzuladen.

    Die Anwendung wird in den Zielordner heruntergeladen, wobei der Fortschritt in der Fortschrittsanzeige angezeigt wird. Wenn der Download abgeschlossen ist, geht der Assistent automatisch zur Seite „Abgeschlossen“ über.
12. Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen.

Hinzufügen eines Core zum Local Mount Utility

Um einen Wiederherstellungspunkt bereitzustellen, müssen Sie einen Core zum Local Mount Utility hinzufügen. Die Anzahl der Cores, die Sie hinzufügen können, ist nicht beschränkt.

Führen Sie die folgenden Schritte aus, um das Local Mount Utility durch Hinzufügen eines Core einzurichten.

So fügen Sie einen Core zum Local Mount Utility hinzu

1 Doppelklicken Sie auf der Maschine, auf der das Local Mount Utility installiert ist, durch Doppelklicken auf das Desktopsymbol.

2 Klicken Sie im Fenster „Benutzerkontensteuerung“ auf **Ja**, damit das Programm Änderungen an der Maschine vornehmen kann.

3 Klicken Sie in der oberen linken Ecke des Fensters „AppAssure Local Mount Utility“ auf **Core hinzufügen**.

4 Geben Sie im Dialogfeld „Core hinzufügen“ die erforderlichen Anmeldeinformationen ein (siehe folgende Tabelle):

Tabelle 33.

Option	Beschreibung
Hostname	Der Name des Core, von dem aus Sie Wiederherstellungspunkte bereitstellen möchten. **HINWEIS:** Wenn Sie das Local Mount Utility in einem Core installieren, fügt das Programm automatisch die lokale Maschine (localhost) hinzu.
Port	Die Portnummer, die zur Kommunikation mit dem Core verwendet wird. Die Standardportnummer ist 8006.
Windows-Benutzer-Anmeldeinformationen verwenden	Wählen Sie diese Option aus, wenn die Anmeldeinformationen für den Zugriff auf den Core mit den Windows-Anmeldeinformationen identisch sind.
Bestimmte Anmeldeinformationen verwenden	Wählen Sie diese Option aus, wenn die Anmeldeinformationen für den Zugriff auf den Core nicht mit den Windows-Anmeldeinformationen identisch sind.
Benutzername	Der Benutzername, der für den Zugriff auf die Core-Maschine verwendet wird. **HINWEIS:** Diese Option ist nur verfügbar, wenn Sie bestimmte Anmeldeinformationen verwenden.
Kennwort	Das Kennwort, das für den Zugriff auf die Core-Maschine verwendet wird. **HINWEIS:** Diese Option ist nur verfügbar, wenn Sie bestimmte Anmeldeinformationen verwenden.

5 Klicken Sie auf **Verbinden**.

6 Wenn Sie mehrere Cores hinzufügen möchten, wiederholen Sie die Schritte Schritt 3 bis Schritt 5 so oft wie erforderlich.

Bereitstellen eines Wiederherstellungspunkts mit dem Local Mount Utility

Vor dem Bereitstellen eines Wiederherstellungspunkts muss das Local Mount Utility (LMU) eine Verbindung zum Core herstellen, auf dem der Wiederherstellungspunkt gespeichert ist. Wie in Hinzufügen eines Core zum Local Mount Utility beschrieben, ist die Anzahl der Cores, die zu LMU hinzugefügt werden können, unbegrenzt. Die Anwendung kann jedoch jeweils nur eine Verbindung zu einem Core herstellen. Wenn Sie beispielsweise einen - Wiederherstellungspunkt eines Agenten bereitstellen, der von einem Core geschützt wird, und dann einen Wiederherstellungspunkt eines Agenten bereitstellen, der von einem anderen Core geschützt wird, wird LMU automatisch vom ersten Core getrennt und eine Verbindung zum zweiten Core hergestellt.

Gehen Sie folgendermaßen vor, um einen Wiederherstellungspunkt auf einem Remote-Core mit dem Local Mount Utility bereitzustellen.

So entfernen Sie die Bereitstellung eines Wiederherstellungspunkts mit dem Local Mount Utility

1. Doppelklicken Sie auf der Maschine, auf der das Local Mount Utility installiert ist, durch Doppelklicken auf das Desktopsymbol.
2. Erweitern Sie im Hauptfenster des AppAssure Local Mount Utility den Core in der Navigationsstruktur, um die geschützten Agenten anzuzeigen.
3. Wählen Sie in der Navigationsstruktur den Agenten aus, von dem ein Wiederherstellungspunkt bereitgestellt werden soll.

   Die Wiederherstellungspunkte werden im Hauptbereich angezeigt.
4. Erweitern Sie den Wiederherstellungspunkt, den Sie bereitstellen möchten, um einzelne Datenträger-Volumes oder Datenbanken anzuzeigen.
5. Klicken Sie mit der rechten Maustaste auf den Wiederherstellungspunkt, den Sie bereitstellen möchten, und wählen Sie eine der folgenden Optionen aus:
   - Bereitstellen
   - Mit Schreibzugriff bereitstellen
   - Schreibgeschützt bereitstellen mit vorherigen Schreibvorgängen
   - Erweiterte Bereitstellung
     a. Geben Sie bei Auswahl von „Erweiterte Bereitstellung“ im Fenster „Erweiterte Bereitstellung“ die in der folgenden Tabelle beschriebenen Optionen an.

Tabelle 34.

Option	Beschreibung
Pfad für Bereitstellungspunkt	Klicken Sie auf die Schaltfläche **Durchsuchen**, um einen anderen Pfad für die Wiederherstellungspunkte als den Standardpfad zum Bereitstellungspunkt auszuwählen.
Bereitstellungstyp	Wählen Sie eine der folgenden Optionen: • Schreibgeschützt bereitstellen • Mit Schreibzugriff bereitstellen • Schreibgeschützt bereitstellen mit vorherigen Schreibvorgängen

   b. Klicken Sie auf **Bereitstellen**.

Das Local Mount Utility öffnet automatisch den Ordner, in dem sich der bereitgestellte Wiederherstellungspunkt befindet.

HINWEIS: Wenn Sie einen bereits bereitgestellten Wiederherstellungspunkt auswählen, werden Sie im Bereitstellungsdialogfeld gefragt, ob Sie die Bereitstellung des Wiederherstellungspunktes aufheben möchten.

Untersuchen eines bereitgestellten Wiederherstellungspunktes mit dem Local Mount Utility

Gehen Sie folgendermaßen vor, um einen Wiederherstellungspunkt zu untersuchen, der in einer früheren Sitzung bereitgestellt wurde und noch bereitgestellt ist.

HINWEIS: Diese Vorgehensweise ist nicht erforderlich, wenn Sie einen Wiederherstellungspunkt direkt nach seiner Bereitstellung untersuchen, da der Ordner, in dem sich der Wiederherstellungspunkt befindet, nach Abschluss des Bereitstellungsvorgangs automatisch geöffnet wird.

So untersuchen Sie einen Wiederherstellungspunkt mit dem Local Mount Utility

1. Doppelklicken Sie auf der Maschine, auf der das Local Mount Utility installiert ist, durch Doppelklicken auf das Desktopsymbol.
2. Klicken Sie im Hauptfenster des Local Mount Utility auf **Aktive Bereitstellungen**.

   Das Fenster „Aktive Bereitstellungen“ wird geöffnet. Darin werden alle bereitgestellten Wiederherstellungspunkte angezeigt.
3. Klicken Sie neben dem Bereitstellungspunkt, aus dem die Wiederherstellung erfolgen soll, auf **Untersuchen**, um den Ordner mit den deduplizierten Volumes zu öffnen.

Aufheben der Bereitstellung eines Wiederherstellungspunkts mit dem Local Mount Utility

Gehen Sie folgendermaßen vor, um die Bereitstellung eines Wiederherstellungspunkts auf einem Remote-Core mit dem Local Mount Utility aufzuheben.

So heben Sie die Bereitstellung eines Wiederherstellungspunkts mit dem Local Mount Utility auf

1. Doppelklicken Sie auf der Maschine, auf der das Local Mount Utility installiert ist, auf das Desktopsymbol für das Local Mount Utility, um das Programm zu starten.
2. Klicken Sie im Hauptfenster des Local Mount Utility auf **Aktive Bereitstellungen**.

   Das Fenster „Aktive Bereitstellungen“ wird geöffnet. Darin werden alle bereitgestellten Wiederherstellungspunkte angezeigt.
3. Führen Sie eine der folgenden Aktionen aus:
   - Um die Bereitstellung eines Wiederherstellungspunkts aufzuheben, wählen Sie den gewünschten Wiederherstellungspunkt aus und klicken Sie dann auf **Bereitstellung aufheben**.
   - Um die Bereitstellung aller Wiederherstellungspunkte aufzuheben, klicken Sie auf **Alle Bereitstellungen aufheben**. Klicken Sie anschließend im Dialogfenster „Alle Bereitstellungen aufheben“ zur Bestätigung auf **Ja**.
4. Schließen Sie das Fenster „Aktive Bereitstellungen“ durch Klicken auf das „X“ in der oberen rechten Ecke.
5. Klicken Sie zum Minimieren der LMU-Anwendung auf das „X“ in der oberen rechten Ecke des Programmfensters.
6. Klicken Sie zum Schließen der LMU-Anwendung mit der rechten Maustaste auf das AppAssure Local Mount Utility-Symbol im LMU-Taskleistenmenü und wählen Sie **Beenden** aus.

Informationen zum Taskleistenmenü des Local Mount Utility

Das LMU-Taskleistenmenü befindet sich in der Taskleiste auf Ihrem Desktop. Klicken Sie mit der rechten Maustaste auf das Symbol, um die verfügbaren Optionen anzuzeigen (siehe Beschreibung in der folgenden Tabelle):

Tabelle 35.

Option	Beschreibung
Wiederherstellungspunkte durchsuchen	Öffnet das LMU-Hauptfenster.
Aktive Bereitstellungen	Öffnet das Dialogfeld „Aktive Bereitstellungen“ über dem LMU-Hauptfenster.
Optionen	Öffnet das Dialogfeld „Optionen“ über dem LMU-Hauptfenster. Im Dialogfeld „Optionen“ können Sie das Standardverzeichnis für Bereitstellungspunkte sowie die Standardanmeldeinformationen des Core für die LMU-Benutzeroberfläche ändern.
Info	Zeigt Lizenzinformationen zum Local Mount Utility an.
Beenden	Schließt die LMU-Anwendung. **HINWEIS:** Wenn Sie auf das X in der oberen Ecke des LMU-Hauptfensters klicken, wird die Anwendung in den Systembereich der Taskleiste minimiert. Die Anwendung wird dadurch nicht beendet.

Verwenden der AppAssure Core- und Agent-Optionen

Wenn Sie mit der rechten Maustaste auf den AppAssure Core oder Agent im LMU-Hauptfenster klicken, können Sie verschiedene Optionen ausführen. Dazu gehören:

- Localhost-Optionen
- Remote-Core-Optionen
- Agent-Optionen

Zugriff auf Localhost-Optionen

Führen Sie den folgenden Schritt aus, um die Localhost-Optionen aufzurufen.

So greifen Sie auf Localhost-Optionen zu

- Klicken Sie mit der rechten Maustaste auf den AppAssure Core oder Agent und klicken Sie auf **Verbindung zu Core erneut herstellen**.

  Die Informationen zum Core werden aktualisiert, z. B. kürzlich hinzugefügte Agenten.

Zugriff auf Remote-Core-Optionen

Führen Sie die folgenden Schritte aus, um die Remote-Core-Optionen aufzurufen.

So greifen Sie auf Remote-Core-Optionen zu

- Klicken Sie mit der rechten Maustaste auf den AppAssure Core oder Agent und wählen Sie dann eine der Remote-Core-Optionen aus, die in der folgenden Tabelle beschrieben sind.

Tabelle 36.

Option	Beschreibung
Verbindung zu Core erneut herstellen	Aktualisiert die Informationen zum Core, z. B. kürzlich hinzugefügte Agenten.
Core entfernen	Löscht den Core aus dem Local Mount Utility.
Core bearbeiten	Öffnet das Fenster „Core bearbeiten“, in dem Sie Hostnamen, Port und Anmeldeinformationen ändern können.

Zugriff auf Agent-Optionen

Führen Sie die folgenden Schritte aus, um die Agent-Optionen aufzurufen.

So greifen Sie auf Agent-Optionen zu

- Klicken Sie mit der rechten Maustaste auf den AppAssure Core oder Agent und klicken Sie auf **Wiederherstellungspunkte aktualisieren**.

  Die Liste der Wiederherstellungspunkte für den ausgewählten Agenten wird aktualisiert.

Verwalten von Aufbewahrungsrichtlinien

Die Anzahl der regelmäßig von allen geschützten Servern erstellten Sicherungs-Snapshots auf dem Core wird im Laufe der Zeit immer größer. Aufbewahrungsrichtlinien werden für die Aufbewahrung von Sicherungs-Snapshots über längere Zeiträume sowie zur Unterstützung bei der Verwaltung dieser Sicherungs-Snapshots verwendet. Eine Aufbewahrungsrichtlinie wird durch einen nächtlichen Rollup-Prozess umgesetzt, der Sie beim Festlegen des Ablaufs und beim Löschen alter Sicherungen unterstützt. Informationen zum Konfigurieren von Aufbewahrungsrichtlinien finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für einen Agenten.

Anleitung für die Archivierung in einer Cloud

Wenn die Daten das Ende eines Aufbewahrungszeitraums erreichen, können Sie die Aufbewahrung verlängern, indem Sie ein Archiv der alten Daten erstellen. Beim Archivieren von Daten stellt sich immer die Frage, wo die Daten gespeichert werden sollen. AppAssure bietet die Möglichkeit, das Archiv direkt in der Core Console in verschiedene Cloud-Anbieter hochzuladen. Kompatible Clouds sind u. a. Windows Azure, Amazon, Rackspace und alle OpenStack-basierten Anbieter.

Der Export eines Archivs in eine Cloud mit AppAssure umfasst die folgenden Verfahren:

- **Cloud-Konto zur AppAssure Core Console hinzufügen.** Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
- **Daten archivieren und in das Cloud-Konto exportieren.** Weitere Informationen finden Sie unter Erstellen eines Archivs.
- **Archivierte Daten durch Importieren vom Cloud-Speicherort abrufen.** Weitere Informationen finden Sie unter Importieren eines Archivs.

Grundlegende Informationen zu Archiven

Aufbewahrungsrichtlinien schreiben den Zeitraum vor, für den Sicherungen auf (schnellen und teuren) Kurzzeitmedien gespeichert werden. Mitunter machen geschäftliche und technische Anforderungen eine längere Aufbewahrung dieser Sicherungen erforderlich. Schnelle Speicher sind jedoch teuer. Deshalb wird durch diese Anforderung (langsame und kostengünstige) Langzeitspeicherung notwendig. Unternehmen verwenden Langzeitspeicher oftmals zur Archivierung

von Compliancedaten und anderen Daten. Mithilfe der Archivierungsfunktion in AppAssure kann der Aufbewahrungszeitraum für Compliancedaten und andere Daten verlängert werden. Außerdem können Sie mit dieser Funktion Replikationsdaten an einen Remote-Replikat-Core übertragen.

Erstellen eines Archivs

Führen Sie die folgenden Schritte aus, um ein Archiv zu erstellen.

So erstellen Sie ein Archiv

1 Navigieren Sie zur AppAssure Core Console und klicken Sie auf die Registerkarte „Extras“.

2 Klicken Sie unter „Archiv“ auf **Erstellen**.

Der Assistent zum Hinzufügen eines Archivs wird geöffnet.

3 Wählen Sie auf der Seite „Erstellen“ des Assistenten zum Hinzufügen eines Archivs eine der folgenden Optionen in der Dropdown-Liste „Typ des Speicherorts“ aus:

- Lokal
- Netzwerk
- Cloud

4 Geben Sie abhängig vom Typ des Speicherorts, der in Schritt 3 ausgewählt wurde, die Details für das Archiv ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 37.

Option	Textfeld	Beschreibung
Lokal	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. D:\Arbeit\Archiv.
Netzwerk	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. \\Servername\Freigabename.
	Benutzername	Geben Sie einen Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **HINWEIS:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname ist „AppAssure-5-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

5 Klicken Sie auf **Weiter**.

6 Wählen Sie auf der Seite „Maschinen“ des Assistenten die geschützten Maschinen mit den zu archivierenden Wiederherstellungspunkten aus.

7 Klicken Sie auf **Weiter**.

8 Geben Sie auf der Seite „Optionen“ die in der folgenden Tabelle beschriebenen Informationen ein.

Textfeld	Beschreibung
Maximale Größe	Umfangreiche Datenarchive können in mehrere Segmente aufgeteilt werden. Wählen Sie den maximalen Speicherplatz aus, der zum Erstellen des Archivs reserviert werden soll. Führen Sie dazu einen der folgenden Schritte aus: • Wählen Sie **Gesamtes Ziel** aus, um den gesamten verfügbaren Speicherplatz im Pfad, der in Schritt 4 für das Ziel angegeben wurde, zu reservieren. (Wenn beispielsweise „D:\Arbeit\Archiv“ als Speicherort angegeben wurde, wird der gesamte verfügbare Speicherplatz auf dem Laufwerk D: reserviert.) • Geben Sie in das leere Textfeld mit den Pfeilen einen Wert ein und wählen Sie dann eine Maßeinheit in der Dropdown-Liste aus, um den maximal reservierten Speicherplatz festzulegen. **HINWEIS:** Archive in der Amazon-Cloud werden automatisch in 50-GB-Segmente aufgeteilt. Archive in der Windows Azure-Cloud werden automatisch in 200-GB-Segmente aufgeteilt.
Recyclingaktion	Wählen Sie eine der folgenden Optionen als Recyclingaktion aus: • **Nicht wiederverwenden.** Vorhandene archivierte Daten am Speicherort werden nicht überschrieben oder gelöscht. Wenn der Speicherort nicht leer ist, können keine Daten in das Archiv geschrieben werden. • **Diesen Core ersetzen.** Alle bereits vorhandenen archivierten Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert. • **Vollständig löschen.** Alle archivierten Daten werden aus dem Verzeichnis gelöscht, bevor das neue Archiv geschrieben wird. • **Inkrementell.** Bietet die Möglichkeit, Wiederherstellungspunkte zu einem vorhandenen Archiv hinzuzufügen. Die Wiederherstellungspunkte werden verglichen, um eine Duplizierung von bereits im Archiv vorhandenen Daten zu vermeiden.
Anmerkung	Geben Sie alle zusätzlich erforderlichen Informationen für die Erfassung des Archivs ein. Die Anmerkung wird angezeigt, wenn Sie das Archiv später importieren.
Kompatibles Format verwenden	Wählen Sie diese Option aus, um die Daten in einem Format zu archivieren, das mit früheren Core-Versionen kompatibel ist. **HINWEIS:** Das neue Format bietet mehr Leistung, ist aber mit älteren Cores nicht kompatibel.

9 Klicken Sie auf **Weiter**.

10 Geben Sie auf der Seite „Datumsbereich“ das Startdatum und das Ablaufdatum der zu archivierenden Wiederherstellungspunkte ein.

- Klicken Sie auf die angezeigte Uhrzeit (Standardwert: 8:00), wenn Sie eine Zeit eingeben möchten, um die Schieberegler für die Auswahl von Stunden und Minuten anzuzeigen.
- Klicken Sie zum Eingeben eines Datums auf das Textfeld, um den Kalender einzublenden, und klicken Sie dann auf den gewünschten Tag.

11 Klicken Sie auf **Fertigstellen**.

Festlegen einer geplanten Archivierung

Mit der Funktion „Geplantes Archiv“ können Sie einen Zeitpunkt festlegen, zu dem automatisch ein Archiv einer ausgewählten Maschine erstellt und am angegebenen Speicherort gespeichert wird. Diese Funktion ist für Situationen vorgesehen, in denen häufig Archive einer Maschine gespeichert werden sollen, ohne dass die Archive jedes Mal manuell erstellt werden müssen. Führen Sie die folgenden Schritte aus, um eine automatische Archivierung zu planen.

So legen Sie eine geplante Archivierung fest

1 Navigieren Sie zur AppAssure Core Console und klicken Sie auf die Registerkarte „Extras“.

2 Klicken Sie unter „Archiv“ auf **Geplant**.

3 Klicken Sie auf der Seite „Geplantes Archiv“ auf **Hinzufügen**.

Der Assistent zum Hinzufügen eines Archivs wird geöffnet.

4 Wählen Sie auf der Seite „Speicherort“ des Assistenten zum Hinzufügen eines Archivs eine der folgenden Optionen in der Dropdown-Liste „Typ des Speicherorts“ aus:

- Lokal
- Netzwerk
- Cloud

5 Geben Sie abhängig vom Typ des Speicherorts, der in Schritt 4 ausgewählt wurde, die Details für das Archiv ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 38.

Option	Textfeld	Beschreibung
Lokal	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. D:\Arbeit\Archiv.
Netzwerk	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. \\Servername\Freigabename.
	Benutzername	Geben Sie einen Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **HINWEIS:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname ist „AppAssure-5-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

6 Klicken Sie auf **Weiter**.

7 Wählen Sie auf der Seite „Geschützte Maschinen“ des Assistenten die geschützten Maschinen mit den zu archivierenden Wiederherstellungspunkten aus.

8 Klicken Sie auf **Weiter**.

9 Wählen Sie auf der Seite „Optionen“ in der Dropdown-Liste eine der folgenden Recyclingaktionen aus:

- **Diesen Core ersetzen.** Alle vorhandenen archivierten Daten auf dem Core werden überschrieben. Die Daten anderer Cores bleiben aber unverändert.
- **Vollständig löschen.** Alle archivierten Daten werden aus dem Verzeichnis gelöscht, bevor das neue Archiv geschrieben wird.
- **Inkrementell.** Bietet die Möglichkeit, Wiederherstellungspunkte zu einem vorhandenen Archiv hinzuzufügen. Die Wiederherstellungspunkte werden verglichen, um eine Duplizierung von bereits im Archiv vorhandenen Daten zu vermeiden.

10 Wählen Sie auf der Seite Zeitplan eine der folgenden Optionen für die Häufigkeit zum Senden von Daten aus:

- Täglich
- Wöchentlich
- Monatlich

11 Geben Sie abhängig von der Auswahl in Schritt 10 die in der folgenden Tabelle beschriebenen Informationen ein.

Option	Textfeld	Beschreibung
Täglich	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der täglich ein Archiv erstellt werden soll.
Wöchentlich	Wochentag	Wählen Sie einen Wochentag aus, an dem das Archiv automatisch erstellt werden soll.
	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der täglich ein Archiv erstellt werden soll.
Monatlich	Tag im Monat	Wählen Sie den Tag im Monat aus, an dem das Archiv automatisch erstellt werden soll.
	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der täglich ein Archiv erstellt werden soll.

12 Wählen Sie **Archivierung zunächst vorübergehend deaktivieren** aus, wenn Sie die Archivierung zunächst vorübergehend deaktivieren, aber später wieder aktivieren möchten.

> **HINWEIS:** Sie können die geplante Archivierung beispielsweise zunächst deaktivieren, wenn Sie den Zielspeicherort vorbereiten müssen, bevor die Archivierung stattfindet. Wenn Sie diese Option nicht auswählen, beginnt die Archivierung zum angegebenen geplanten Zeitpunkt.

13 Klicken Sie auf **Fertigstellen**.

Deaktivieren oder Aktivieren einer geplanten Archivierung

Bisweilen kann es vorkommen, dass Sie einen geplanten Archivierungsjob vorübergehend deaktivieren müssen, z. B. wenn der Zielspeicherort für das Archiv geändert werden muss. Wenn die Archivierung bei der Durchführung der in Festlegen einer geplanten Archivierung beschriebenen Schritte vorübergehend deaktiviert wurde, soll die geplante Archivierung ebenso zu einem späteren Zeitpunkt wieder aktiviert werden. Führen Sie die folgenden Schritte aus, um eine geplante Archivierung vorübergehend zu deaktivieren und wieder zu aktivieren.

So deaktivieren oder aktivieren Sie eine geplante Archivierung

1 Navigieren Sie zur AppAssure Core Console und klicken Sie auf die Registerkarte „Extras“.

2 Klicken Sie unter „Archiv“ auf **Geplant**.

3 Führen Sie auf der Seite „Geplantes Archiv“ eine der folgenden Aktionen aus:

- Wählen Sie das gewünschte Archiv aus und klicken Sie dann auf eine der folgenden Aktionen:
  - Vorübergehend deaktivieren
  - Wieder aktivieren
- Klicken Sie neben dem gewünschten Archiv im Dropdown-Menü auf eine der folgenden Aktionen:
  - Vorübergehend deaktivieren
  - Wieder aktivieren

Der Status des Archivs wird in der Spalte „Zeitplan“ angezeigt.

Bearbeiten einer geplanten Archivierung

Sie können in AppAssure die Details einer geplanten Archivierung ändern. Führen Sie die nachstehend beschriebenen Schritte aus, um eine geplante Archivierung zu bearbeiten.

So bearbeiten Sie eine geplante Archivierung

1 Navigieren Sie zur AppAssure Core Console und klicken Sie auf die Registerkarte „Extras“.

2 Klicken Sie unter „Archiv“ auf **Geplant**.

3 Klicken Sie auf der Seite „Geplantes Archiv“ auf das Dropdown-Menü neben der dem Archiv, das geändert werden soll, und klicken Sie dann auf **Bearbeiten**.

Der Assistent zum Hinzufügen eines Archivs wird geöffnet.

4 Wählen Sie auf der Seite „Speicherort“ des Assistenten zum Hinzufügen eines Archivs eine der folgenden Optionen in der Dropdown-Liste „Typ des Speicherorts“ aus:

- Lokal
- Netzwerk
- Cloud

5 Geben Sie abhängig vom Typ des Speicherorts, der in Schritt 4 ausgewählt wurde, die Details für das Archiv ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 39.

Option	Textfeld	Beschreibung
Lokal	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. D:\Arbeit\Archiv.
Netzwerk	Ausgabespeicherort	Geben Sie den Speicherort für die Ausgabe ein. Damit wird der Pfad festgelegt, in dem das Archiv gespeichert werden soll, z. B. \\Servername\Freigabename.
	Benutzername	Geben Sie einen Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie ein Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **HINWEIS:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie einen Namen für den Ordner ein, in dem die archivierten Daten gespeichert werden sollen. Der Standardname ist „AppAssure-5-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

6 Klicken Sie auf **Weiter**.

7 Wählen Sie auf der Seite „Geschützte Maschinen“ des Assistenten die geschützten Maschinen mit den zu archivierenden Wiederherstellungspunkten aus.

8 Klicken Sie auf **Weiter**.

9 Wählen Sie auf der Seite Zeitplan eine der folgenden Optionen für die Häufigkeit zum Senden von Daten aus:

- Täglich

- Wöchentlich
- Monatlich

10 Geben Sie abhängig von der Auswahl in Schritt 9 die in der folgenden Tabelle beschriebenen Informationen ein.

Option	Textfeld	Beschreibung
Täglich	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der täglich ein Archiv erstellt werden soll.
Wöchentlich	Wochentag	Wählen Sie einen Wochentag aus, an dem das Archiv automatisch erstellt werden soll.
	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der täglich ein Archiv erstellt werden soll.
Monatlich	Tag im Monat	Wählen Sie den Tag im Monat aus, an dem das Archiv automatisch erstellt werden soll.
	Uhrzeit	Wählen Sie die Uhrzeit aus, zu der täglich ein Archiv erstellt werden soll.

11 Wählen Sie **Archivierung zunächst vorübergehend deaktivieren** aus, wenn Sie die Archivierung zunächst vorübergehend deaktivieren, aber später wieder aktivieren möchten.

> **HINWEIS:** Sie können die geplante Archivierung beispielsweise zunächst deaktivieren, wenn Sie den Zielspeicherort vorbereiten müssen, bevor die Archivierung stattfindet. Wenn Sie diese Option nicht auswählen, beginnt die Archivierung zum angegebenen geplanten Zeitpunkt.

12 Klicken Sie auf **Fertigstellen**.

Überprüfen eines Archivs

Sie können die strukturelle Integrität eines Archivs überprüfen, indem Sie eine Archivprüfung durchführen. Bei dieser Prüfung wird festgestellt, ob alle erforderlichen Dateien im Archiv vorhanden sind. Führen Sie die nachstehend beschriebenen Schritte aus, um eine Archivprüfung durchzuführen.

So überprüfen Sie ein Archiv

1 Navigieren Sie zur AppAssure Core Console und klicken Sie auf die Registerkarte „Extras“.

2 Klicken Sie unter „Archiv“ auf **Archiv prüfen**.

3 Das Dialogfeld „Archiv prüfen“ wird angezeigt.

4 Wählen Sie in der Dropdown-Liste **Typ des Speicherorts** eine der folgenden Optionen aus:

- Lokal
- Netzwerk
- Cloud

5 Geben Sie abhängig vom Typ des Speicherorts, der in Schritt 4 ausgewählt wurde, die Details für das Archiv ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 40.

Option	Textfeld	Beschreibung
Lokal	Speicherort	Geben Sie das Kennwort für das Archiv ein.

Tabelle 40.

Option	Textfeld	Beschreibung
Netzwerk	Speicherort	Geben Sie das Kennwort für das Archiv ein.
	Benutzername	Geben Sie den Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie das Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. HINWEIS: Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie den Namen des Ordners ein, in dem die archivierten Daten gespeichert sind, z. B. „AppAssure-5-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

6 Wählen Sie **Strukturintegrität** aus, wenn auch eine Überprüfung der Strukturintegrität durchgeführt werden soll.

7 Klicken Sie auf **Datei überprüfen**.

Importieren eines Archivs

Wenn Sie archivierte Daten wiederherstellen möchten, müssen Sie das gesamte Archiv an einen angegebenen Speicherort importieren. Anschließend können Sie die Daten durchsuchen. Führen Sie die nachstehend beschriebenen Schritte aus, um ein Archiv zu importieren.

So importieren Sie ein Archiv

1 Navigieren Sie zur AppAssure Core Console und wählen Sie die Registerkarte „Extras“ aus.

2 Klicken Sie unter „Archiv“ auf **Importieren**.

3 Wählen Sie in der Dropdown-Liste **Typ des Speicherorts** eine der folgenden Optionen aus:

- Lokal
- Netzwerk
- Cloud

4 Geben Sie abhängig vom Typ des Speicherorts, der in Schritt 3 ausgewählt wurde, die Details für das Archiv ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 41.

Option	Textfeld	Beschreibung
Lokal	Speicherort	Geben Sie das Kennwort für das Archiv ein.
Netzwerk	Speicherort	Geben Sie das Kennwort für das Archiv ein.
	Benutzername	Geben Sie den Benutzernamen ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.
	Kennwort	Geben Sie das Kennwort für den Netzwerkpfad ein. Diese Angabe wird als Anmeldeinformation für die Netzwerkfreigabe verwendet.

Tabelle 41.

Option	Textfeld	Beschreibung
Cloud	Konto	Wählen Sie ein Konto in der Dropdown-Liste aus. **HINWEIS:** Um ein Cloud-Konto auswählen zu können, müssen Sie das Konto zuerst in der Core Console hinzufügen. Weitere Informationen finden Sie unter Hinzufügen eines Cloud-Kontos.
	Container	Wählen Sie im Dropdown-Menü einen Container für das Konto aus.
	Ordnername	Geben Sie den Namen des Ordners ein, in dem die archivierten Daten gespeichert sind, z. B. „AppAssure-5-Archive-[ERSTELLUNGSDATUM]-[ERSTELLUNGSZEIT]“.

5 Klicken Sie auf **Datei prüfen**, um festzustellen, ob das zu importierende Archiv vorhanden ist.

6 Überprüfen Sie im Dialogfenster den Namen des in der Dropdown-Liste „Core“ angezeigten Quell-Core.

7 Wählen Sie die Agenten aus, die aus dem Archiv importiert werden sollen.

8 Wählen Sie das Repository aus, in dem die archivierten Daten gespeichert werden sollen.

HINWEIS: Das ausgewählte Repository muss das Repository sein, in dem alle aktuellen Wiederherstellungspunkte für den ausgewählten Agenten gespeichert sind.

9 Klicken Sie auf **Wiederherstellen**, um das Archiv zu importieren.

Verwalten von SQL-Anfügbarkeit und Protokollkürzung

Mit der Konfiguration der SQL-Anfügbarkeit kann der AppAssure Core unter Verwendung einer lokalen Instanz von Microsoft SQL Server SQL-Datenbank- und Protokolldateien in einem Snapshot eines SQL-Servers anfügen. Mithilfe der Anfügbarkeitsprüfung kann der Core die Konsistenz der SQL-Datenbanken prüfen und sicherstellen, dass alle Datendateien (MDF- und LDF-Dateien) im Sicherungs-Snapshot verfügbar sind. Anfügbarkeitsprüfungen können bei Bedarf für bestimmte Wiederherstellungspunkte oder im Rahmen nächtlicher Jobs ausgeführt werden.

Die Anfügbarkeit setzt voraus, dass eine lokale Microsoft SQL Server-Instanz auf der AppAssure Core-Maschine vorhanden ist. Diese Instanz muss eine volllizenzierte SQL Server-Version sein, die bei Microsoft oder einem lizenzierten Händler erworben wurde. Microsoft lässt keine Nutzung von passiven SQL-Lizenzen zu.

Die Anfügbarkeit wird für SQL Server 2005, 2008, 2008 R2, 2012 und 2014 unterstützt. Das für den Test verwendete Konto muss über die sysadmin-Rolle für die SQL Server-Instanz verfügen.

Das SQL Server-Speicherformat auf der Festplatte ist in den 64-Bit- und 32-Bit-Umgebungen identisch, sodass die Anfügbarkeit in beiden Versionen funktioniert. Eine Datenbank, die von einer in einer Umgebung aktiven Serverinstanz getrennt wurde, kann an eine in einer anderen Umgebung aktive Serverinstanz angefügt werden.

Bei der Protokollkürzung wird der in den SQL-Datenbankprotokollen verfügbare Speicherplatz ermittelt, aber nicht minimiert. Sie können die Protokollkürzung so einrichten, dass sie im Rahmen der nächtlichen Jobs erfolgt, oder bei Bedarf durchführen. Informationen zum Erzwingen einer Protokollkürzung finden Sie unter Erzwingen einer Protokollkürzung für eine SQL- oder Exchange-Maschine

HINWEIS: Die SQL Server-Version auf dem Core muss gleich oder höher als die SQL Server-Version auf allen Agent-Maschinen sein, auf denen SQL Server installiert ist.

In diesem Abschnitt werden folgende Themen behandelt:

- Konfigurieren der SQL-Anfügbarkeitseinstellungen
- Konfigurieren von nächtlichen SQL-Anfügbarkeitsprüfungen und Protokollkürzungen für alle geschützten Maschinen

Weitere Informationen zur Verwaltung von Maschinen mit SQL Server finden Sie unter Ändern von SQL Server-Einstellungen bzw. Anpassen der nächtlichen Jobs für eine geschützte Maschine.

Konfigurieren der SQL-Anfügbarkeitseinstellungen

Damit Sie Anfügbarkeitsprüfungen für geschützte SQL-Datenbanken durchführen können, müssen Sie zuerst eine lokale SQL Server-Instanz auf der Core-Maschine auswählen, die für die Durchführung der Prüfungen auf der Agent-Maschine verwendet wird.

HINWEIS: Die Anfügbarkeit setzt voraus, dass eine lokale Microsoft SQL Server-Instanz auf der AppAssure Core-Maschine vorhanden ist. Diese Instanz muss eine volllizenzierte SQL Server-Version sein, die bei Microsoft oder einem lizenzierten Händler erworben wurde. Microsoft lässt keine Nutzung von passiven SQL-Lizenzen zu.

Führen Sie die folgenden Schritte aus, um SQL-Anfügbarkeitseinstellungen zu konfigurieren.

So konfigurieren Sie SQL-Anfügbarkeitseinstellungen

1. Navigieren Sie zum AppAssure Core und klicken Sie auf die Registerkarte „Konfiguration“.
2. Klicken Sie auf **Einstellungen**.
3. Klicken Sie im Bereich „Nächtliche Jobs“ auf **ändern**.

   Das Dialogfeld „Nächtliche Jobs“ wird angezeigt.
4. Wählen Sie **Anfügbarkeitsprüfjob** aus und klicken Sie dann auf **Einstellungen**.

   Daraufhin wird das Dialogfeld „Konfiguration“ angezeigt, in dem Sie die lokale SQL Server-Instanz für die Durchführung der Anfügbarkeitsprüfung für geschützte SQL Server-Datenbanken auswählen können.
5. Sie können im Dropdown-Menü über die folgenden Optionen die SQL Server-Instanz auswählen, die im Core installiert ist:
   - SQL Server 2005
   - SQL Server 2008
   - SQL Server 2008 R2
   - SQL Server 2012
   - SQL Server 2014

   HINWEIS: Die jeweils in diesem Dropdown-Menü angezeigten Optionen hängen von den jeweiligen lokalen SQL Server-Instanzen in der Umgebung ab.
6. Wählen Sie die Art der Anmeldeinformationen aus. Sie haben folgende Auswahlmöglichkeiten:
   - Windows oder
   - SQL
7. Geben Sie die Anmeldeinformationen mit Administratorberechtigungen für die Windows- oder SQL Server-Instanzen ein (siehe Beschreibung in der folgenden Tabelle).

   Tabelle 42.

Textfeld	Beschreibung
Benutzername	Geben Sie einen Benutzernamen mit Anmeldeberechtigung beim SQL-Server ein.
Kennwort	Geben Sie ein Kennwort für die SQL-Anfügbarkeit ein. Dieses wird zur Steuerung der Anmeldeaktivität verwendet.

8. Klicken Sie auf **Verbindung testen**.

   HINWEIS: Wenn Sie die Anmeldeinformationen falsch eingegeben haben, wird eine Meldung mit dem Hinweis angezeigt, dass die Überprüfung der Anmeldeinformationen fehlgeschlagen ist. Korrigieren Sie die Anmeldeinformationen und führen Sie den Verbindungstest erneut aus.
9. Klicken Sie auf **Speichern**.

Für die geschützten SQL Server-Datenbanken können jetzt Anfügbarkeitsprüfungen durchgeführt werden.

10 Klicken Sie im Bereich „Nächtliche Jobs“ auf **OK**.

Die Anfügbarkeitsprüfungen werden jetzt planmäßig im Rahmen der nächtlichen Jobs angezeigt.

Konfigurieren von nächtlichen SQL-Anfügbarkeitsprüfungen und Protokollkürzungen für alle geschützten Maschinen

Im Dialogfeld „Nächtliche Jobs“, das über den Core erreichbar ist, können Sie SQL-Datenbankservereinstellungen, z. B. Anfügbarkeitsprüfung und nächtliche Protokollkürzung, anzeigen, aktivieren oder deaktivieren. Die hier vorgenommenen Änderungen gelten für alle durch den Core geschützten SQL-Maschinen.

Führen Sie die folgenden Schritte aus, damit das System nächtliche Anfügbarkeitsprüfungen für die SQL Server-Wiederherstellungspunkte durchführt.

So konfigurieren Sie nächtliche SQL-Anfügbarkeitsprüfungen und Protokollkürzungen

1 Navigieren Sie zum AppAssure Core und klicken Sie auf die Registerkarte „Konfiguration“.

2 Klicken Sie auf **Einstellungen**.

3 Klicken Sie im Abschnitt „Nächtliche Jobs“ auf **Ändern**.

4 Wählen Sie abhängig von den jeweiligen Anforderungen der Organisation die folgenden SQL Server-Einstellungen aus oder ab:

- Anfügbarkeitsprüfjob
- Protokollkürzungsjob (nur einfaches Wiederherstellungsmodell)

5 Klicken Sie auf **OK**.

Die Einstellungen für Anfügbarkeit und Protokollkürzung werden für den geschützten SQL Server wirksam.

Verwalten von Bereitstellbarkeitsprüfungen und Protokollkürzung für Exchange-Datenbanken

Wenn Sie AppAssure für die Sicherung von Microsoft Exchange-Servern verwenden, können nach jedem Snapshot für alle Exchange-Datenbanken Bereitstellbarkeitsprüfungen durchgeführt werden. Diese Funktion ermöglicht die Ermittlung von Beschädigungen. Sie weist Administratoren auf mögliche Fehler hin und stellt sicher, dass alle Daten auf den Exchange-Servern bei einem Ausfall erfolgreich wiederhergestellt werden.

Bei der Protokollkürzung wird die Größe der Protokolle einer Exchange-Datenbank täglich minimiert (falls deren Ausführung im Rahmen der nächtlichen Jobs geplant ist). Informationen zum Erzwingen der Protokollkürzung finden Sie unter Erzwingen einer Protokollkürzung für eine SQL- oder Exchange-Maschine.

HINWEIS: Bereitstellbarkeitsprüfungen sind nur für Microsoft Exchange 2007, 2010 und 2013 relevant. Außerdem muss das AppAssure Agent-Dienstkonto über die Rolle als Organisationsadministrator in Exchange verfügen.

Weitere Informationen zur Verwaltung von Maschinen mit Exchange Server finden Sie unter Verwalten von Exchange- und SQL Server-Maschinen.

Konfigurieren von nächtlichen Prüfsummenprüfungen und Protokollkürzungen für Exchange-Datenbanken

Auf der Konfigurationsregisterkarte auf Core-Ebene können Sie Exchange-Datenbankservereinstellungen anzeigen, aktivieren oder deaktivieren, z. B. automatische Bereitstellbarkeitsprüfungen, nächtliche Prüfsummenprüfungen oder nächtliche Protokollkürzungen. Die auf dieser Registerkarte vorgenommenen Änderungen gelten für alle durch den Core geschützten Exchange-Maschinen.

Führen Sie die folgenden Schritte aus, um die Einstellungen für Bereitstellbarkeit und Protokollkürzung von Exchange-Datenbanken zu konfigurieren.

So konfigurieren Sie Bereitstellbarkeitsprüfungen und Protokollkürzungen für Exchange-Datenbanken

1. Navigieren Sie zum AppAssure Core und klicken Sie auf die Registerkarte „Konfiguration“.
2. Klicken Sie auf **Einstellungen**.
3. Klicken Sie im Abschnitt „Nächtliche Jobs“ auf **Ändern**.
4. Wählen Sie abhängig von den jeweiligen Anforderungen der Organisation die folgenden Exchange Server-Einstellungen aus oder ab:
   - Prüfsummenprüfjob
   - Exchange-Protokolle kürzen
5. Klicken Sie auf **OK**.

   Die Einstellungen für Prüfsummen und Protokollkürzung werden für den geschützten Exchange-Server wirksam.

   HINWEIS: Informationen zum Erzwingen der Protokollkürzung finden Sie unter Erzwingen einer Protokollkürzung für eine SQL- oder Exchange-Maschine.

Statusanzeigen für Wiederherstellungspunkte

Wenn ein Wiederherstellungspunkt für einen geschützten SQL- oder Exchange-Server erstellt wurde, zeigt die Anwendung den Status in der Tabelle der Wiederherstellungspunkte in der entsprechenden Farbe an. Die angezeigte Farbe hängt von den Überprüfungseinstellungen für die geschützte Maschine und dem Ergebnis dieser Überprüfungen (Erfolg bzw. Fehlschlag) ab (siehe Beschreibung in den folgenden Tabellen zur Statusfarbe von Wiederherstellungspunkten für SQL-Datenbanken sowie für Exchange-Datenbanken).

HINWEIS: Weitere Informationen zum Anzeigen von Wiederherstellungspunkten finden Sie unter Anzeigen von Wiederherstellungspunkten.

Statusfarbe von Wiederherstellungspunkten für SQL-Datenbanken

Die folgende Tabelle enthält eine Liste der Statusanzeigen für SQL-Datenbanken.

Tabelle 43.

Statusfarbe	Beschreibung
Weiß	Zeigt an, das eine der folgenden Bedingungen besteht: • Eine SQL-Datenbank war nicht vorhanden. • Anfügbarkeitsprüfungen wurden nicht aktiviert. • Anfügbarkeitsprüfungen wurden noch nicht durchgeführt.
Gelb	Zeigt an, dass die SQL-Datenbank offline und eine Überprüfung nicht möglich war.

Tabelle 43.

Statusfarbe	Beschreibung
Rot	Zeigt an, dass die Anfügbarkeitsprüfung fehlgeschlagen ist.
Grün	Zeigt an, dass die Anfügbarkeitsprüfung erfolgreich war.

Statusfarbe von Wiederherstellungspunkten für Exchange-Datenbanken

Die folgende Tabelle enthält eine Liste der Statusanzeigen für Exchange-Datenbanken.

Tabelle 44.

Statusfarbe	Beschreibung
Weiß	Zeigt an, das eine der folgenden Bedingungen besteht: • Eine Exchange-Datenbank war nicht vorhanden. • Bereitstellbarkeitsprüfungen wurden nicht aktiviert. **HINWEIS:** Dies kann für bestimmte Volumes innerhalb eines Wiederherstellungspunktes gelten.
Gelb	Zeigt an, dass Bereitstellbarkeitsprüfungen für die Exchange-Datenbank aktiviert sind, die Überprüfungen aber noch nicht durchgeführt wurden.
Rot	Zeigt an, dass die Bereitstellbarkeitsprüfungen oder die Prüfsummenprüfungen für mindestens eine Datenbank fehlgeschlagen sind.
Grün	Zeigt an, dass die Bereitstellbarkeitsprüfung bzw. die Prüfsummenprüfung erfolgreich war.

HINWEIS: Wiederherstellungspunkte, denen keine Exchange- oder SQL-Datenbank zugeordnet ist, werden mit einer weißen Statusanzeige angezeigt. In Situationen, in denen es für den Wiederherstellungspunkt sowohl eine Exchange- als auch eine SQL-Datenbank gibt, wird die schwerwiegendste Statusanzeige für den Wiederherstellungspunkt angezeigt.

3

Schützen von Arbeitsstationen und Servern

In diesem Kapitel wird beschrieben, wie die Agent-Maschinen in der AppAssure-Umgebung geschützt, konfiguriert und verwaltet werden. Folgende Themen werden behandelt:

- Informationen zum Schützen von Arbeitsstationen und Servern
- Informationen zu Schutzzeitplänen
- Schützen einer Maschine
- Konfigurieren von Maschineneinstellungen
- Anzeigen von Systemdiagnoseinformationen
- Verwalten von Core-Jobeinstellungen
- Bereitstellen eines Agenten (Push-Installation)
- Verwalten von Maschinen
- Verwalten mehrerer Maschinen
- Verwalten von Snapshots und Wiederherstellungspunkten
- Verwalten von SQL- und Exchange-Servern
- Informationen zum Wiederherstellen von Daten aus Wiederherstellungspunkten
- Information zum Exportieren geschützter Daten von Windows-Maschinen in virtuelle Maschinen
- Grundlegende Informationen zur BMR-Wiederherstellung
- Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen
- Verwalten eines Windows-Start-Image
- Starten einer BMR-Wiederherstellung für Linux
- Überprüfen einer BMR-Wiederherstellung
- Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen
- Verwalten eines Linux-Start-Image
- Verwalten von Linux-Partitionen
- Starten einer BMR-Wiederherstellung für Linux
- Überprüfen der BMR-Wiederherstellung über die Befehlszeile
- Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen

Informationen zum Schützen von Arbeitsstationen und Servern

Um Ihre Daten mit AppAssure zu schützen, müssen Sie die zu schützenden Arbeitsstationen und Server, z. B. Exchange-Server, SQL Server, Linux-Server usw., zur AppAssure Core Console hinzufügen.

HINWEIS: In diesem Kapitel bezieht sich das Wort *Maschine* im Allgemeinen auch auf die AppAssure Agent-Software, die auf der jeweiligen Maschine installiert ist.

In der AppAssure Core Console können Sie die Maschine angeben, auf der ein AppAssure Agent installiert ist und angeben, welche Volumes, z. B. ein Microsoft Windows-Speicherplatz, geschützt werden sollen. Sie können Schutzzeitpläne festlegen, weitere Schutzmaßnahmen hinzufügen, z. B. Verschlüsselung, usw. Weitere Informationen zum Öffnen der AppAssure Core Console zum Schützen von Arbeitsstationen und Servern finden Sie unter Schützen einer Maschine.

Einschränkungen bei der Unterstützung dynamischer Volumes und Basis-Volumes

AppAssure unterstützt die Erstellung von Snapshots aller dynamischer Volumes und Basis-Volumes. Darüber hinaus unterstützt AppAssure den Export von einfachen dynamischen Volumes, die sich auf einem einzelnen physischen Datenträger befinden. Wie der Name impliziert, sind einfache dynamische Volumes keine Stripeset-Volumes, gespiegelte Volumes oder übergreifende Volumes.

Dynamische Datenträger (außer den bereits erwähnten, einfachen dynamischen Datenträgern) stehen im Exportassistenten nicht zur Auswahl zur Verfügung. Nicht einfache dynamische Volumes weisen beliebige Datenträgergeometrien auf, die nicht vollständig ausgewertet werden können. AppAssure bietet daher keine Möglichkeit, komplexe oder nicht einfache dynamische Volumes zu exportieren.

In der Benutzeroberfläche wird eine Benachrichtigung mit dem Hinweis angezeigt, dass Exportvorgänge nur eingeschränkt möglich und auf einfache dynamische Volumes beschränkt sind. Wenn Sie versuchen, ein anderes Volume als einzelnes dynamisches Volume zu exportieren, schlägt der Exportjob fehl.

Informationen zu Schutzzeitplänen

Ein Schutzzeitplan legt fest, wann Sicherungen von geschützten Agent-Maschinen zum AppAssure Core übertragen werden.

Die Schutzzeitpläne werden zunächst mit den Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen definiert. Sie können bestehende Zeitpläne jederzeit auf der Registerkarte „Zusammenfassung“ für eine bestimmte Agent-Maschine ändern.

HINWEIS: Informationen zum Schützen einer einzelnen Maschine finden Sie unter Schützen einer Maschine. Informationen zum Massenschutz (Schützen mehrerer Maschinen) finden Sie unter Schützen mehrerer Maschinen. Informationen um Anpassen von Schutzzeiträumen beim Schützen eines Agenten mit einem der beiden Assistenten finden Sie unter Erstellen benutzerdefinierter Schutzzeitpläne. Informationen zum Ändern eines bestehenden Schutzzeitplans finden Sie unter Ändern von Schutzzeitplänen.

AppAssure umfasst einen Standardschutzzeitplan mit zwei Schutzzeiträumen. Der erste Zeitraum gilt an Wochentagen (Montag bis Freitag) mit einem einzigen Zeitraum (von 00:00 bis 23:59 Uhr). Das Standardintervall (der Zeitabstand zwischen Snapshots) beträgt 60 Minuten.

Der zweite Zeitraum gilt an Wochenenden (Samstag und Sonntag). Das Standardintervall beträgt ebenfalls 60 Minuten.

Wenn der Schutz erstmals aktiviert wird, wird auch der Zeitplan aktiviert. So wird mit den Standardeinstellungen die erste Sicherung unabhängig von der Tageszeit zu jeder vollen Stunde durchgeführt (00:00, 01:00, 02:00 usw.).

Die erste übertragene Sicherung, die im Core gespeichert wird, heißt Basisimage-Snapshot. Alle Daten auf allen angegebenen Volumes (einschließlich Betriebssystem, Anwendungen und Einstellungen) werden im Core gespeichert. Danach werden regelmäßig inkrementelle Snapshots (kleinere Sicherungen, die nur die seit der letzten Sicherung geänderten Daten auf dem Agenten umfassen) im festgelegten Zeitintervall (z. B. alle 60 Minuten) auf dem Core gespeichert.

Sie können einen benutzerdefinierten Zeitplan erstellen, um die Häufigkeit der Sicherungen zu ändern. Einen einfache Änderung, die Sie beispielsweise vornehmen können, besteht darin, das Intervall für Wochentage in 20 Minuten zu ändern, sodass jede Stunde drei Snapshots erstellt werden. Sie können auch das Intervall an Wochenenden von 60 Minuten auf 180 Minuten, sodass alle drei Stunden Snapshots erstellt werden, wenn der Verkehrsaufkommen gering ist.

Sie können für Wochentage auch Spitzennutzungszeiten und Zeiten mit geringer Auslastung definieren. Ändern Sie dazu mit dem Assistenten für Schutzzeitpläne die Standardstart- und -endzeit in einen kleineren Bereich (z. B. 08:00 bis 16:59) und legen Sie ein geeignetes Intervall fest (z. B. 20 Minuten). In diesen Spitzennutzungszeiten werden häufig Sicherungen erstellt.

Wählen Sie dann **Restliche Zeit Snapshots erstellen** aus und geben Sie ein geeignetes (größeres) Intervall an (z. B. 180 Minuten). Diese Einstellungen legen Zeiten mit geringer Auslastung fest - alle Zeiträume von Montags bis Freitag außerhalb der Spitzennutzungszeiten. Snapshots werden dann von 00:00 bis 7:59 und von 17:00 bis 23:59 alle 3 Stunden erstellt.

Weitere Optionen auf der Seite „Schutzzeitplan“ des Assistenten ermöglichen die Festlegung einer täglichen Schutzzeit. Zum festgelegten Zeitpunkt (Standardeinstellung: 12:00 Uhr) wird dann täglich eine einzelne Sicherung durchgeführt.

Die Option, den Schutz zunächst vorübergehend zu deaktivieren, verhindert, dass ein Basisimage erstellt wird, sodass keinerlei Sicherung erfolgt, bis der Schutz wieder explizit aktiviert werden. Wenn der Schutz der Maschinen gemäß dem eingerichteten Schutzzeitplan gestartet werden kann, müssen Sie den Schutz explizit wieder aktivieren. Weitere Informationen zum erneuten Aktivieren der Schutzfunktion finden Sie unter Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion. Wenn eine Maschine sofort geschützt werden soll, können Sie ggf. einen Snapshot erzwingen. Weitere Informationen finden Sie unter Erzwingen eines Snapshots.

Schützen einer Maschine

In diesem Abschnitt wird beschrieben, wie der Schutz der Daten für eine einzelne Maschine gestartet wird, die Sie im Assistenten zum Schützen einer Maschine angeben.

> **HINWEIS:** Auf der Maschine muss die AppAssure Agent-Software installiert sein, damit sie geschützt werden kann. Sie können die Agent-Software installieren, bevor Sie die nachstehend beschriebenen Schritte ausführen, oder die Software im Rahmen der Durchführung des Assistenten zum Schützen einer Maschine bereitstellen. Weitere Informationen zum Installieren der Agent-Software finden Sie unter „Installation von Agenten auf Windows-Maschinen“ im *Dell AppAssure Bereitstellungshandbuch*.
>
> Wenn die Agent-Software nicht installiert wurde, bevor eine Maschine geschützt wird, können Sie im Assistenten nicht bestimmte Volumes auswählen, die geschützt werden sollen. In diesem Fall werden standardmäßig alle Volumes auf der Agent-Maschine unter Schutz gestellt.
>
> AppAssure unterstützt Schutz und Wiederherstellung von Maschinen mit EISA-Partitionen. Die Unterstützung wurde auch auf Maschinen mit Windows 8 und 8.1 sowie Windows 2012 und 2012 R2 erweitert, die Windows RE (Windows Recovery Environment) verwenden.

Informationen zum Schützen mehrerer Maschinen gleichzeitig finden Sie unter Schützen mehrerer Maschinen.

Wenn Sie eine Maschine unter Schutz stellen, müssen Sie Verbindungsinformationen wie IP-Adresse und Port festlegen und Anmeldeinformationen für die zu schützende Maschine angeben. Optional können Sie einen Anzeigenamen eingeben, der in der Core Console anstelle der IP-Adresse angezeigt wird. Sie legen auch den Schutzzeitplan für die Maschine fest.

Dieser Prozess umfasst optionale Schritte, auf die Sie zugreifen können, wenn Sie eine erweiterte Konfiguration auswählen, z. B. Hinzufügen eines neuen oder Angeben eines vorhandenen Repositorys sowie ggf. Verschlüsseln der im Core für die jeweilige Maschine gespeicherten Daten.

Der Workflow des Assistenten kann abhängig von der jeweiligen Umgebung geringfügig abweichen. Wenn beispielsweise die Agent-Software auf der zu schützenden Maschine installiert ist, werden Sie im Assistenten nicht aufgefordert, die Software zu installieren. Ebenso werden Sie nicht aufgefordert, ein Repository zu erstellen, wenn im Core bereits ein Repository vorhanden ist.

So schützen Sie eine Maschine

1 Starten Sie die Maschine neu, wenn die AppAssure Agent-Software auf der zu schützenden Maschine bereits installiert, die Maschine aber noch nicht neu gestartet wurde.

2 Navigieren Sie auf der Core-Maschine zur AppAssure Core Console und klicken Sie in der Schaltflächenleiste auf **Schützen**.

Der Assistent zum Schützen einer Maschine wird angezeigt.

3 Wählen Sie auf der Begrüßungsseite die gewünschten Installationsoptionen aus:

- Wählen Sie **Standard** aus, wenn Sie kein Repository definieren und keine Verschlüsselung einrichten müssen.
- Wählen Sie **Erweitert (optionale Schritte anzeigen)** aus, wenn Sie ein Repository erstellen, ein anderes Repository für Sicherungen der ausgewählten Maschine angeben oder die Verschlüsselung mit dem Assistenten einrichten müssen.
- Sie können die Option **Diese Begrüßungsseite beim nächsten Start des Assistenten überspringen** auswählen, wenn die Begrüßungsseite des Assistenten zum Schützen einer Maschine nicht mehr angezeigt werden soll.

4 Wenn Sie die gewünschten Optionen auf der Begrüßungsseite festgelegt haben, klicken Sie auf **Weiter**.

Die Seite „Verbindung“ wird angezeigt.

5 Geben Sie auf der Seite „Verbindung“ die in der folgenden Tabelle beschriebenen Verbindungsinformationen für die Maschine ein und klicken Sie dann auf **Weiter**.

Tabelle 45.

Textfeld	Beschreibung
Host	Der Hostname oder die IP-Adresse der Maschine, die Sie schützen möchten.
Port	Die Nummer des Ports, über den der AppAssure Core mit dem Agenten auf der Maschine kommuniziert. Die Standardportnummer ist 8006.
Benutzername	Der Benutzername für die Verbindung zu dieser Maschine, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Das Kennwort, das für die Verbindung zu dieser Maschine verwendet wird.

6 Wechseln Sie zu Schritt 7, wenn als Nächstes die Seite „Schutz“ im Assistenten angezeigt wird.

Wenn im Assistenten als Nächstes die Seite „Agent installieren“ angezeigt wird, wurde die Agent-Software noch nicht auf der jeweiligen Maschine installiert. Klicken Sie auf **Weiter**, um die Agent-Software zu installieren.

> **HINWEIS:** Die Agent-Software muss auf der zu schützenden Maschine installiert sein und die Maschine muss neu gestartet worden sein, damit sie im Core gesichert werden kann. Wählen Sie die Option **Maschine nach der Installation automatisch neu starten (empfohlen)** aus, bevor Sie auf **Weiter** klicken, damit das Installationsprogramm die Agent-Maschine neu startet.

Die Seite „Schutz“ wird angezeigt.

7 Wenn in der AppAssure Core Console anstelle der IP-Adresse ein Name für die Agent-Maschine angezeigt werden soll, können Sie im Feld „Anzeigename“ des Dialogfelds einen Namen eingeben.

Sie können bis zu 64 Zeichen eingeben.

8 Wählen Sie den gewünschten Schutzzeitplan aus (siehe nachstehende Beschreibung).

- Wählen Sie unter „Zeitplaneinstellungen“ die Option **Standardschutz (stündliche Snapshots aller Volumes)** aus, um den Standardschutzzeitplan zu verwenden.

  Im Standardschutzzeitplan erstellt der Core jede Stunde Snapshots der Agent-Maschine. Auf der Registerkarte „Zusammenfassung“ für die jeweilige Agent-Maschine können Sie jederzeit die Schutzeinstellungen ändern, nachdem der Assistent beendet wurde, z. B. die zu schützenden Volumes auswählen.

- Wählen Sie unter „Zeitplaneinstellungen“ die Option **Benutzerdefinierter Schutz** aus, um einen anderen Schutzzeitplan zu definieren.

9 Setzen Sie die Konfiguration wie folgt fort:

- Klicken Sie auf **Fertigstellen**, wenn Sie im Assistenten die Standardkonfiguration und Standardschutz ausgewählt haben, um die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebene Maschine zu schützen.
- Wenn eine Maschine erstmals unter Schutz gestellt wird, wird ein Basisimage (ein Snapshot aller Daten in den geschützten Volumes) an das Repository im AppAssure Core übertragen (dem festgelegten Zeitplan entsprechend) - es sei denn, Sie haben angegeben, dass der Schutz vorübergehend deaktiviert werden soll.
- Klicken Sie auf **Weiter**, wenn Sie im Assistenten die Standardkonfiguration und benutzerdefinierten Schutz ausgewählt haben, um einen benutzerdefinierten Schutzzeitplan einzurichten. Ausführliche Informationen zum Festlegen eines benutzerdefinierten Schutzzeitplans finden Sie unter Erstellen benutzerdefinierter Schutzzeitpläne.
- Klicken Sie auf **Weiter**, wenn Sie im Assistenten die erweiterte Konfiguration und Standardschutz ausgewählt haben, und gehen Sie zu Schritt Schritt 12, um Repository- und Verschlüsselungsoptionen anzugeben.
- Klicken Sie auf **Weiter**, wenn Sie im Assistenten die erweiterte Konfiguration und benutzerdefinierten Schutz ausgewählt haben, und gehen Sie zu Schritt Schritt 10, um die zu schützenden Volumes anzugeben.

10 Wählen Sie auf der Seite „Schutz-Volumes“ die Volumes auf der Agent-Maschine aus, die Sie schützen möchten. Klicken Sie in der Spalte „Überprüfen“ auf die aufgelisteten Volumes, die nicht geschützt werden sollen, um die Auswahl aufzuheben. Klicken Sie anschließend auf **Weiter**.

> **HINWEIS:** In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

11 Legen Sie auf der Seite „Schutzzeitplan“ einen benutzerdefinierten Schutzzeitplan fest.

12 Führen Sie auf der Seite „Repository“ eine der folgenden Aktionen aus:

- Wählen Sie **Vorhandenes Repository verwenden** aus, wenn die zu schützenden Daten der Maschine in einem vorhandenen Repository gespeichert werden sollen, wählen Sie das entsprechende Repository in der Liste aus, und klicken Sie dann auf **Weiter**.

  Die Seite „Verschlüsselung“ wird angezeigt. Wechseln Sie zu Schritt 17, um ggf. Verschlüsselungseinstellungen zu definieren.

- Gehen Sie folgendermaßen vor, um einen neuen Speicherort im Core zu erstellen:

  a Wählen Sie **Repository erstellen** aus.

  b Geben Sie auf der Seite „Repository“ im Feld **Name** den Namen des Repositorys an, das Sie erstellen möchten.

  Das Feld enthält normalerweise das Wort „Repository“ sowie eine Indexnummer, die der Nummer des neuen Repositorys entspricht (z. B. **Repository1**). Sie können den Namen bei Bedarf ändern. Sie können bis zu 40 Zeichen eingeben. Der Name muss für den Core eindeutig sein.

HINWEIS: Verwenden Sie im Repositorynamen nur alphanumerische Zeichen und Bindestriche. Andere Symbole oder Interpunktionszeichen sind nicht zulässig. Verwenden Sie keine Buchstabenkombinationen, die mit Befehlen oder reservierten Wörtern übereinstimmen (z. B. con, prn, aux oder nul) oder Anschlüsse darstellen (z. B. com oder lpt).

c Geben Sie im **Speicherort** einen Verzeichnispfad für das Repository ein. Geben Sie beispielsweise für ein Repository auf einem lokalen Computer **C:\Repository** ein. Der Speicherort muss für den Core eindeutig sein. Geben Sie das Repository im Format \\Servername\Freigabename an, wenn das Repository in einem freigegebenen Laufwerk gespeichert werden soll.

VORSICHT: Wenn Sie das Repository später löschen, entfernt das Installationsprogramm alle Inhalte im Repositorypfad. Erstellen Sie den Speicherort deshalb nicht im Stammverzeichnis (z. B. c:\), da dann alle auf dem betreffenden Volume gespeicherten Daten verloren gehen können.

d Geben Sie im Feld **Benutzername** einen Benutzernamen mit Zugriffsberechtigungen für das freigegeben Laufwerk und im Feld **Kennwort** das Kennwort für diesen Benutzer ein, wenn das Repository auf einem freigegebenen Volume gespeichert wird.

e Geben Sie im Feld **Metadatenpfad** den Pfad ein, in dem Metadaten gespeichert werden sollen. Dies sollte in Unterverzeichnis des Speicherorts sein. Geben Sie beispielsweise **C:\Repository\Metadata** ein, wenn C:\Repository als Speicherort angegeben wurde. Der Pfad muss für den Core eindeutig sein.

13 Klicken Sie auf **Weiter**, wenn Sie alle erforderlichen Daten auf der Seite „Repository“ angegeben haben.

Die Seite „Repository-Konfiguration“ wird angezeigt.

14 Geben Sie die Größe des Repositorys ein.

HINWEIS: Wenn es sich beim Speicherort um ein NTFS-Volume (New Technology File System) unter Windows XP oder Windows 7 handelt, ist die Dateigröße auf 16 TB beschränkt.

Wenn es sich beim Speicherort um ein NTFS-Volume (New Technology File System) unter Windows 8, 8.1 oder Windows Server 2012, 2012 R2 handelt, ist die Dateigröße auf 256 TB beschränkt.

Damit AppAssure das Betriebssystem überprüfen kann, muss die Windows-Verwaltungsinstrumentation (WMI) auf dem beabsichtigten Speicherort installiert sein.

15 Wählen Sie **Erweiterte Optionen anzeigen** aus, um die Bytes pro Sektor oder die Bytes pro Datensatz anzugeben bzw. die Schreib-Caching-Richtlinie festzulegen, und geben Sie dann die in der folgenden Tabelle beschriebenen Details für den Speicherort ein.

Tabelle 46.

Textfeld	Beschreibung
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist *512*.

Tabelle 46.

Textfeld	Beschreibung
Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist *8192*.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung *Ein* steuert Windows das Caching. **HINWEIS:** Wenn die Schreib-Caching-Richtlinie auf *Ein* festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie eine Version von Windows Server vor Server 2012, ist die empfohlene Einstellung *Aus*. Bei Auswahl von *Aus* steuert AppAssure das Caching. Bei Auswahl von *Sync* steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.

16 Wenn Sie die gewünschten Informationen für die Repositorykonfiguration eingegeben haben, klicken Sie auf **Weiter**.

Die Seite „Verschlüsselung“ wird angezeigt.

17 Wählen Sie ggf. auf der Seite „Verschlüsselung“ die Option **Verschlüsselung aktivieren** aus, um die Verschlüsselung zu aktivieren.

Daraufhin werden auf der Seite „Verschlüsselung“ Felder für Verschlüsselungsschlüssel angezeigt.

HINWEIS: Wenn Sie die Verschlüsselung aktivieren, werden die Daten aller geschützten Volumes für die jeweilige Agent-Maschine verschlüsselt.

Sie können die Einstellungen später auf der Registerkarte „Konfiguration“ in der AppAssure Core Console ändern.

Weitere Informationen zur Verschlüsselung finden Sie im Abschnitt Verwalten der Sicherheit.

VORSICHT: AppAssure verwendet 256-Bit-AES-Verschlüsselung im CBC-Modus (Cipher Block Chaining) mit 256-Bit-Schlüsseln. Obwohl die Verwendung der Verschlüsselung optional ist, wird von Dell dringend empfohlen, einen Verschlüsselungsschlüssel einzurichten und die festgelegte Passphrase zu schützen. Speichern Sie die Passphrase an einem sicheren Speicherort, da sie für die Datenwiederherstellung von entscheidender Bedeutung ist. Ohne Passphrase ist keine Datenwiederherstellung möglich.

18 Geben Sie die in der folgenden Tabelle beschriebenen Informationen ein, um einen Verschlüsselungsschlüssel für den Core hinzuzufügen.

Tabelle 47.

Textfeld	Beschreibung
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein.
Beschreibung	Geben Sie eine Beschreibung mit weiteren Details für den Verschlüsselungsschlüssel ein.
Passphrase	Geben Sie die Passphrase für die Zugriffssteuerung ein.
Passphrase wiederholen	Geben Sie zuvor eingegebene Passphrase erneut ein.

19 Klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und zu übernehmen.

Wenn eine Maschine erstmals unter Schutz gestellt wird, wird ein Basisimage (ein Snapshot aller Daten in den geschützten Volumes) an das Repository im AppAssure Core übertragen (dem festgelegten Zeitplan entsprechend) - es sei denn, Sie haben angegeben, dass der Schutz vorübergehend deaktiviert werden soll.

Erstellen benutzerdefinierter Schutzzeitpläne

Wenn Sie die Schutzfunktion mit den Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen konfigurieren, müssen Sie einen Schutzzeitplan festlegen.

Der Standardschutzzeitplan umfasst zwei Schutzzeiträume: einen für Wochentage und einen für Wochenenden. Der Standardzeitbereich für beide ist 00:00 bis 23:59 Uhr (voller 24-Stunden-Tag). Das Standardschutzintervall für beide Schutzzeiträume beträgt 60 Minuten.

Mit dem Assistenten können Sie Schutzzeitpläne anpassen, indem Sie die gewünschten Zeiträume auswählen oder eine tägliche Schutzzeit angeben.

Wenn Sie Zeiträume auswählen, wird der Standardschutzzeitplan angezeigt, den Sie je nach Bedarf anpassen können. Wenn Sie eine tägliche Schutzzeit auswählen, sichert AppAssure die angegebenen geschützten Maschinen einmal täglich zur angegebenen Uhrzeit.

Wenn Sie Zeiträume verwenden, können Sie den Standardschutzzeitplan ohne großen Aufwand ändern. Sie können beispielsweise das Intervall im Standardzeitplan für Wochentage in 20 Minuten, sodass Sicherungen drei Mal stündlich anstatt ein Mal stündlich durchgeführt werden.

Sie können auch komplexere Schutzzeitpläne erstellen. Sie können beispielsweise Spitzennutzungszeiten und Zeiten mit geringer Auslastung für Wochentage erstellen (siehe Beschreibung in Informationen zu Schutzzeitplänen).

Wenn Sie Maschinen mit dem Assistenten schützen, können Sie den Schutz zunächst vorübergehend deaktivieren, d. h., Sie können den Schutzzeitplan festlegen, ohne die Schutzfunktion zu starten. Wenn der Schutz der Maschinen gemäß dem eingerichteten Schutzzeitplan gestartet werden kann, müssen Sie den Schutz explizit wieder aktivieren. Weitere Informationen zum erneuten Aktivieren der Schutzfunktion finden Sie unter Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion. Wenn eine Maschine sofort geschützt werden soll, können Sie ggf. einen Snapshot erzwingen. Weitere Informationen finden Sie unter Erzwingen eines Snapshots.

HINWEIS: Konzeptionelle Informationen zu Schutzzeitplänen finden Sie unter Informationen zu Schutzzeitplänen. Informationen zum Schützen einer einzelnen Maschine finden Sie unter Schützen einer Maschine. Informationen zum Massenschutz (Schützen mehrerer Maschinen) finden Sie unter Schützen mehrerer Maschinen. Informationen um Anpassen von Schutzzeiträumen beim Schützen eines Agenten mit einem der beiden Assistenten finden Sie unter Erstellen benutzerdefinierter Schutzzeitpläne. Informationen zum Ändern eines bestehenden Schutzzeitplans finden Sie unter Ändern von Schutzzeitplänen.

Führen Sie die nachstehend beschriebenen Schritte aus, um Zeitpläne für den Schutz der Daten auf Agent-Maschinen zu erstellen, wenn Sie die Schutzfunktion mit einem Assistenten einrichten.

So erstellen Sie benutzerdefinierte Zeitpläne

1. Führen Sie die folgenden Schritte aus, um auf der Seite „Schutzzeitplan“ der Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen den Intervallzeitplan für einen Zeitraum zu ändern:
   a. Wählen Sie **Zeiträume** aus.

      Die bestehenden Zeiträume werden angezeigt und können geändert werden. Sie können für jeden Zeitraum Startzeit, Endzeit und Intervall (in Minuten) in den entsprechenden Feldern bearbeiten.

   b. Klicken Sie in das Intervallfeld und geben Sie das gewünschte Intervall in Minuten ein.

      Markieren Sie beispielsweise das bestehende Intervall und ersetzten Sie den Wert durch den Wert **20**, sodass in diesem Zeitraum alle 20 Minuten Snapshots erstellt werden.

2 Um Spitzennutzungszeiten und Zeiten geringer Auslastung für Wochentage zu erstellen, ändern Sie den Zeitbereich des Zeitraums für Wochentage so, dass kein 24-Stunden-Zeitraum abgedeckt wird. Legen Sie ein optimales Intervall für Spitzennutzungszeiten fest, wählen Sie **Restliche Zeit Snapshots erstellen** aus und legen Sie ein Intervall für Zeiten mit geringer Auslastung fest. Gehen Sie dazu folgendermaßen vor:

   a Wählen Sie **Zeiträume** aus.

   Die bestehenden Zeiträume werden angezeigt und können geändert werden.

   b Klicken Sie in das Feld **Von**, um die Anfangszeit für diesen Zeitraum zu ändern.

   Das Dialogfeld „Zeit auswählen“ wird angezeigt.

   c Ziehen Sie die Schieberegler für Stunden und Minuten auf die gewünschte Startzeit und klicken Sie auf **Fertig**. Klicken Sie auf **Jetzt**, um die aktuelle Uhrzeit anzugeben.

   Ziehen Sie das Steuerelement „Stunden“ beispielsweise auf 08:00 Uhr.

   d Klicken Sie in das Feld **Bis**, um die Endzeit für diesen Zeitraum zu ändern.

   Das Dialogfeld „Zeit auswählen“ wird angezeigt.

   e Ziehen Sie die Schieberegler für Stunden und Minuten auf die gewünschte Startzeit und klicken Sie auf **Fertig**. Klicken Sie auf **Jetzt**, um die aktuelle Uhrzeit anzugeben.

   Ziehen Sie das Steuerelement „Stunden“ beispielsweise auf 16:59 Uhr.

3 Wählen Sie **Tägliche Schutzzeit** aus, wenn täglich zu einer bestimmten Uhrzeit eine Sicherung durchgeführt werden soll, und geben Sie eine Uhrzeit im Format HH:MM AM ein. Geben Sie beispielsweise 9:00 PM ein, wenn täglich um 21:00 Uhr eine Sicherung durchgeführt werden soll.

4 Wählen Sie **Schutz zunächst vorübergehend deaktivieren** aus, um den Zeitplan zu definieren, ohne dass Sicherungen gestartet werden.

   Wenn Sie den Schutz im Assistenten vorübergehend deaktiviert haben, bleibt dieser so lange deaktiviert, bis Sie ihn explizit wieder aktivieren. Wenn der Schutz wieder aktiviert wird, werden Sicherungen gemäß dem eingerichteten Zeitplan durchgeführt. Weitere Informationen zum erneuten Aktivieren der Schutzfunktion finden Sie unter Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion.

5 Klicken Sie auf **Fertigstellen** bzw. **Weiter**, wenn der Schutzzeitplan wie gewünscht geändert wurde. Kehren Sie zur Vorgehensweise des jeweiligen Assistenten zurück, um weitere erforderliche Einstellungen zu konfigurieren.

Ändern von Schutzzeitplänen

Ein Schutzzeitplan legt fest, wann Sicherungen von geschützten Agent-Maschinen zum AppAssure Core übertragen werden. Die Schutzzeitpläne werden zunächst mit den Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen definiert.

Sie können bestehende Schutzzeitpläne jederzeit auf der Registerkarte „Zusammenfassung“ für eine bestimmte Agent-Maschine ändern.

> **HINWEIS:** Konzeptionelle Informationen zu Schutzzeitplänen finden Sie unter Informationen zu Schutzzeitplänen. Informationen zum Schützen einer einzelnen Maschine finden Sie unter Schützen einer Maschine. Informationen zum Massenschutz (Schützen mehrerer Maschinen) finden Sie unter Schützen mehrerer Maschinen. Informationen um Anpassen von Schutzzeiträumen beim Schützen eines Agenten mit einem der beiden Assistenten finden Sie unter Erstellen benutzerdefinierter Schutzzeitpläne. Informationen zum Ändern eines bestehenden Schutzzeitplans finden Sie unter Ändern von Schutzzeitplänen.

Führen Sie die folgenden Schritte aus, um einen bestehenden Schutzzeitplan für die Volumes einer geschützten Maschine zu ändern.

So ändern Sie Schutzzeitpläne

1 Navigieren Sie zur AppAssure Core Console.

2 Wählen Sie in der Liste der geschützten Maschinen die Maschine mit dem Schutzzeitplan aus, den Sie ändern möchten.

Die Registerkarte „Zusammenfassung“ für die Maschine wird angezeigt.

3 Wählen Sie die Volumes für die geschützte Maschine aus, die geändert werden sollen, und klicken Sie auf **Zeitplan festlegen**. Klicken Sie auf das Kontrollkästchen in der Kopfzeile, um alle Volumes gleichzeitig auszuwählen.

Zunächst wird derselbe Schutzzeitplan für alle Volumes verwendet. In der Regel sollten zumindest das Volume „System-reserviert“ und das Volume mit dem Betriebssystem (normalerweise Laufwerk C:) geschützt werden.

Das Dialogfeld „Schutzzeitplan“ wird angezeigt.

4 Wählen Sie im Dialogfeld „Schutzzeitplan“ die gewünschte Vorlage in der Dropdown-Liste aus, wenn Sie zuvor eine Schutzzeitplanvorlage erstellt haben, die für den jeweiligen Agenten verwendet werden soll, und wechseln Sie zu Schritt 10.

5 Geben Sie in das Textfeld einen Vorlagennamen ein, wenn dieser neue Schutzzeitplan als Vorlage gespeichert werden soll.

6 Deaktivieren Sie die Kontrollkästchen neben den einzelnen Zeitraumoptionen, um einen bestehenden Zeitraum aus dem Zeitplan zu entfernen. Folgende Optionen sind verfügbar:

- **Mo - Fr:** Dieser Zeitraum deckt eine normale 5-Tage-Arbeitswoche ab.
- **Sa - So:** Dieser Zeitraum deckt ein normales Wochenende ab.

7 Wenn Start- und Endzeit für Wochentage auf 00:00 bis 23:59 eingestellt sind, ist nur ein Zeitraum vorhanden. Gehen Sie folgendermaßen vor, um Start- oder Endzeit eines festgelegten Zeitraums zu ändern:

a Wählen Sie den entsprechenden Zeitraum aus.

b Klicken Sie in das Feld **Startzeit**, um die Anfangszeit für diesen Zeitraum zu ändern.

Das Dialogfeld „Zeit auswählen“ wird angezeigt.

c Ziehen Sie die Schieberegler für Stunden und Minuten auf die gewünschte Startzeit und klicken Sie auf **Fertig**. Klicken Sie auf **Jetzt**, um die aktuelle Uhrzeit anzugeben.

Ziehen Sie das Steuerelement „Stunden“ beispielsweise auf 08:00 Uhr.

d Klicken Sie in das Feld **Endzeit**, um die Endzeit für diesen Zeitraum zu ändern.

Das Dialogfeld „Zeit auswählen“ wird angezeigt.

e Ziehen Sie die Schieberegler für Stunden und Minuten auf die gewünschte Startzeit und klicken Sie auf **Fertig**. Klicken Sie auf **Jetzt**, um die aktuelle Uhrzeit anzugeben.

Ziehen Sie das Steuerelement „Stunden“ beispielsweise auf 16:59 Uhr.

f Ändern Sie das Intervall den jeweiligen Anforderungen entsprechend. Ändern Sie beispielsweise das Intervall für Spitzenzeiten von 60 Minuten in 20 Minuten, damit jede Stunde drei Snapshots erstellt werden.

8 Wenn Sie in Schritt 7 einen anderen Zeitraum als 00:00 bis 23:59 festgelegt haben und in der restlichen Zeit Sicherungen erstellt werden sollen, müssen Sie weitere Schutzzeiträume hinzufügen. Gehen Sie dazu folgendermaßen vor:

a Klicken Sie auf **Zeitraum hinzufügen**.

Unter der jeweiligen Kategorie (Wochentage oder Wochenenden) wird ein neuer Zeitraum angezeigt. Wenn der erste Zeitraum später als 00:00 Uhr beginnt, wird in AppAssure automatisch ein Zeitraum hinzugefügt, der um 00:00 beginnt. Im vorliegenden Beispiel beginnt der zweite Zeitraum um 00:00. Sie müssen die Stunden- oder Minutenangaben für Start- und Endzeiten u. U. anpassen.

b Ziehen Sie die Schieberegler für Stunden und Minuten auf die gewünschte Start- und Endzeit.

Legen Sie beispielsweise eine Startzeit von 00:00 und eine Endzeit von 07:59 fest.

c Ändern Sie das Intervall den jeweiligen Anforderungen entsprechend. Ändern Sie beispielsweise das Intervall für Zeiten geringer Auslastung von 60 Minuten in 120 Minuten, damit alle zwei Stunden in Snapshot erstellt wird.

9 Erstellen Sie bei Bedarf weitere Zeiträume. Legen Sie dazu die gewünschten Start- und Endzeiten sowie Intervalle fest.

HINWEIS: Klicken Sie auf das **X** ganz rechts für einen Zeitraum, um einen hinzugefügten Zeitraum zu löschen. Wenn Sie einen Zeitraum irrtümlich entfernt haben, können Sie auf **Abbrechen** klicken.

10 Klicken Sie auf **Übernehmen**, wenn der Schutzzeitplan Ihre Anforderungen erfüllt.

Das Dialogfeld „Schutzzeitplan“ wird geschlossen.

Verwalten von Exchange- und SQL Server-Maschinen

In der AppAssure Core Console werden spezielle Optionen für Exchange Server und SQL Server angezeigt, wenn eine Instanz der Software und die zugehörigen Datenbanken auf geschützten Servern festgestellt werden. Dieser Abschnitt umfasst spezielle Themen für die Verwaltung von Maschinen mit Exchange Server oder SQL Server.

In diesem Abschnitt werden folgende Themen behandelt:

- Ändern von Exchange Server-Einstellungen
- Erzwingen einer Bereitstellbarkeitsprüfung für eine Exchange-Datenbank
- Erzwingen von Prüfsummenprüfungen für Exchange Server-Wiederherstellungspunkte
- Ändern von SQL Server-Einstellungen
- Erzwingen einer SQL Server-Anfügbarkeitsprüfung
- Erzwingen einer Protokollkürzung für eine SQL- oder Exchange-Maschine

Ändern von Exchange Server-Einstellungen

Wenn Sie Daten eines Microsoft Exchange-Servers schützen möchten, müssen Sie weitere Einstellungen in der AppAssure Core Console konfigurieren.

So ändern Sie Exchange Server-Einstellungen

1 Nachdem Sie die Exchange Server-Maschine unter Schutz gestellt haben, gehen Sie zur AppAssure Core Console und wählen Sie die Maschine im Navigationsbereich aus.

Die Registerkarte „Zusammenfassung“ für die Maschine wird angezeigt.

2 Klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü **Aktionen** auf **Exchange** und wählen Sie im kontextsensitiven Dropdown-Menü die gewünschte Aktion aus.

- Klicken Sie auf **Protokollkürzung erzwingen**, wenn Sie die Exchange-Serverprotokolle kürzen möchten.
- Klicken Sie auf **Anmeldeinformationen einrichten**, wenn Sie die Anmeldeinformationen für einen einzelnen Exchange-Server festlegen möchten, und führen Sie im Dialogfeld „Exchange-Anmeldeinformationen bearbeiten“ die folgenden Schritte aus:

f Geben Sie im Textfeld „Benutzername“ den Benutzernamen eines Benutzers mit Berechtigungen für den Exchange-Server ein, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).

g Geben Sie im Textfeld „Kennwort“ das Kennwort für den Benutzernamen ein, der für die Verbindung zum Exchange-Server angegeben wurde.

h Klicken Sie auf **OK** um die Einstellungen zu bestätigen und das Dialogfeld zu schließen.

Erzwingen einer Bereitstellbarkeitsprüfung für eine Exchange-Datenbank

Führen Sie die folgenden Schritte aus, damit das System eine Bereitstellbarkeitsprüfung für einen bestimmten Exchange Server-Wiederherstellungspunkt durchführt.

HINWEIS: Damit eine Bereitstellbarkeitsprüfung durchgeführt werden kann, muss auf einem geschützten Volume eine Exchange-Datenbank vorhanden sein. Falls AppAssure nicht feststellen kann, dass eine Datenbank vorhanden ist, wird die Bereitstellbarkeitsprüffunktion nicht in der Core Console angezeigt.

So erzwingen Sie eine Bereitstellbarkeitsprüfung

1. Wählen Sie im linken Navigationsbereich der AppAssure Core Console die Maschine aus, für die Sie eine Bereitstellbarkeitsprüfung erzwingen möchten, und klicken Sie dann auf die Registerkarte **Wiederherstellungspunkte**.
2. Klicken Sie auf das Symbol mit der rechten spitzen Klammer > neben einem Wiederherstellungspunkt in der Liste, um die Ansicht zu erweitern.
3. Klicken Sie auf **Überprüfen** und dann auf **Bereitstellbarkeitsprüfung erzwingen**.

   Daraufhin wird ein Popup-Fenster mit der Frage angezeigt, ob Sie eine Bereitstellbarkeitsprüfung erzwingen möchten.
4. Klicken Sie auf **Ja**.

   Das System führt die Bereitstellbarkeitsprüfung durch.

   HINWEIS: Informationen zum Anzeigen des Status der Bereitstellbarkeitsprüfung finden Sie unter Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen.

Erzwingen von Prüfsummenprüfungen für Exchange Server-Wiederherstellungspunkte

Führen Sie die folgenden Schritte aus, damit das System eine Prüfsummenprüfung für einen bestimmten Exchange Server-Wiederherstellungspunkt durchführt.

HINWEIS: Damit eine Prüfsummenprüfung durchgeführt werden kann, muss auf einem geschützten Volume eine Exchange-Datenbank vorhanden sein. Falls AppAssure nicht feststellen kann, dass eine Datenbank vorhanden ist, wird die Prüfsummenprüffunktion nicht in der Core Console angezeigt.

So erzwingen Sie eine Prüfsummenprüfung

1. Wählen Sie im linken Navigationsbereich der AppAssure Core Console die Maschine aus, für die Sie eine Prüfsummenprüfung erzwingen möchten, und klicken Sie dann auf die Registerkarte **Wiederherstellungspunkte**.
2. Klicken Sie auf das Symbol mit der rechten spitzen Klammer > neben einem Wiederherstellungspunkt in der Liste, um die Ansicht zu erweitern.
3. Klicken Sie auf **Überprüfen** und dann auf **Prüfsummenprüfung erzwingen**.

   Das Fenster „Prüfsummenprüfung erzwingen“ wird mit der Frage angezeigt, ob Sie eine Prüfsummenprüfung erzwingen möchten.
4. Klicken Sie auf **Ja**.

   Das System führt die Prüfsummenprüfung durch.

   HINWEIS: Informationen zum Anzeigen des Status der Anfügbarkeitsprüfung finden Sie unter Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen.

Ändern von SQL Server-Einstellungen

Wenn Sie Microsoft SQL Server-Daten schützen möchten, müssen Sie weitere Einstellungen in der AppAssure Core Console konfigurieren.

So ändern Sie SQL Server-Einstellungen

1. Nachdem Sie die SQL Server-Maschine unter Schutz gestellt haben, gehen Sie zur AppAssure Core Console und wählen Sie die Maschine im Navigationsbereich aus.

   Die Registerkarte „Zusammenfassung“ für die Maschine wird angezeigt.

2. Klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü **Aktionen** auf „SQL“ und wählen Sie im kontextsensitiven Dropdown-Menü die gewünschte Aktion aus.

   - Klicken Sie auf **Protokollkürzung erzwingen**, wenn Sie die SQL- oder Exchange-Serverprotokolle kürzen möchten.
   - Klicken Sie auf **Standardanmeldeinformationen für alle Instanzen festlegen**, wenn Sie die Standardanmeldeinformationen für alle SQL Server-Datenbankinstanzen festlegen möchten, und führen Sie im Dialogfeld „Standardanmeldeinformationen bearbeiten“ die folgenden Schritte aus:

     a. Geben Sie im Textfeld „Benutzername“ den Benutzernamen eines Benutzers mit Berechtigungen für alle SQL-Server ein, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).

     b. Geben Sie im Textfeld „Kennwort“ das Kennwort für den Benutzernamen ein, der für die Verbindung zum SQL-Server angegeben wurde.

     c. Klicken Sie auf **OK** um die Einstellungen zu bestätigen und das Dialogfeld zu schließen.

   - Klicken Sie auf **Anmeldeinformationen für Instanz festlegen**, wenn Sie die Anmeldeinformationen für eine einzelne SQL Server-Datenbankinstanz festlegen möchten, und führen Sie im Dialogfeld „Anmeldeinformationen für Instanz bearbeiten“ die folgenden Schritte aus:

     a. Wählen Sie den Typ der Anmeldeinformationen aus („Standard“, „Windows“ oder „SQL“).

     b. Geben Sie im Textfeld „Benutzername“ den Benutzernamen eines Benutzers mit Berechtigungen für den SQL-Server ein, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).

     c. Geben Sie im Textfeld „Kennwort“ das Kennwort für den Benutzernamen ein, der für die Verbindung zum SQL-Server angegeben wurde.

     d. Klicken Sie auf **OK** um die Einstellungen zu bestätigen und das Dialogfeld zu schließen.

Erzwingen einer SQL Server-Anfügbarkeitsprüfung

Führen Sie die folgenden Schritte aus, damit das System eine Anfügbarkeitsprüfung für einen bestimmten SQL Server-Wiederherstellungspunkt durchführt.

HINWEIS: Damit eine Anfügbarkeitsprüfung durchgeführt werden kann, muss auf einem geschützten Volume eine SQL-Datenbank vorhanden sein. Falls AppAssure nicht feststellen kann, dass eine Datenbank vorhanden ist, wird die Anfügbarkeitsprüffunktion nicht in der Core Console angezeigt.

So erzwingen Sie eine SQL Server-Anfügbarkeitsprüfung

1. Wählen Sie im linken Navigationsbereich des AppAssure Core die Maschine aus, für die Sie eine Anfügbarkeitsprüfung erzwingen möchten, und klicken Sie dann auf die Registerkarte **Wiederherstellungspunkte**.
2. Klicken Sie auf das Symbol mit der rechten spitzen Klammer > neben einem Wiederherstellungspunkt in der Liste, um die Ansicht zu erweitern.
3. Klicken Sie auf **Überprüfen** und dann auf **Anfügbarkeitsprüfung erzwingen**.

   Das Fenster „Anfügbarkeitsprüfung erzwingen“ wird mit der Frage angezeigt, ob Sie eine Anfügbarkeitsprüfung erzwingen möchten.

4 Klicken Sie auf **Ja**.

Das System führt die Anfügbarkeitsprüfung durch.

HINWEIS: Informationen zum Anzeigen des Status der Anfügbarkeitsprüfung finden Sie unter Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen.

Erzwingen einer Protokollkürzung für eine SQL- oder Exchange-Maschine

Die Protokollkürzung ist für Maschinen mit SQL Server oder Exchange Server verfügbar. Führen Sie die folgenden Schritte aus, um eine Protokollkürzung zu erzwingen.

HINWEIS: Wird die Protokollkürzung für eine Exchange-Maschine durchgeführt, wird die Größe der Protokolle verringert. Bei einer SQL-Maschine wird der freie Speicherplatz auf einem Datenträger ermittelt, die Größe der Protokolle aber nicht verringert.

So erzwingen Sie eine Protokollkürzung

1 Navigieren Sie in der AppAssure Core Console zu der geschützten Maschine, für die Sie eine Protokollkürzung erzwingen möchten.

2 Klicken Sie auf der Registerkarte „Zusammenfassung“ der geschützten Maschine in das Dropdown-Menü **Aktionen** und führen Sie dann eine der folgenden Aktionen durch:

- Wählen Sie **SQL** aus, wenn die geschützte Maschine SQL Server verwendet, und klicken Sie dann auf **Protokollkürzung erzwingen**.
- Wählen Sie **Exchange** aus, wenn die geschützte Maschine Exchange Server verwendet, und klicken Sie dann auf **Protokollkürzung erzwingen**.

3 Klicken Sie auf **Ja**, um zu bestätigen, dass die Protokollkürzung durchgeführt werden soll.

Anpassen der nächtlichen Jobs für eine geschützte Maschine

Nächtliche Jobs können auf der jeweiligen Konfigurationsregisterkarte auf Core-Ebene bzw. auf Maschinenebene konfiguriert werden. Werden die Einstellungen für nächtliche Jobs auf der Core-Ebene geändert, gelten die Änderungen für alle relevanten Maschinen, die durch den betreffenden Core geschützt werden. Änderungen der nächtlichen Jobs, die auf Maschinenebene durchgeführt werden, überschreiben die auf der Core-Ebene vorgenommenen Änderungen.

Führen Sie die nachstehend beschrieben Schritte aus, um die nächtlichen Jobs für eine einzelne Maschine zu ändern.

So passen Sie die nächtlichen Jobs für eine geschützte Maschine an

1 Wählen Sie im linken Navigationsbereich des AppAssure Core die Maschine aus, für die Sie die nächtlichen Jobs anpassen möchten.

Die Registerkarte „Zusammenfassung“ für die ausgewählte Maschine wird angezeigt.

2 Klicken Sie auf die Registerkarte „Konfiguration“ für die Maschine und dann auf **Einstellungen**.

3 Klicken Sie neben „Nächtliche Jobs“ auf **ändern**.

Das Dialogfeld „Nächtliche Jobs“ wird angezeigt.

4 Wählen Sie die Jobs, die als nächtliche Jobs ausgeführt werden sollen, oder deaktivieren Sie die Optionen, die für die betreffende Maschine nicht verwendet werden sollen.

HINWEIS: Die Optionen hängen von der jeweiligen Maschine ab. Eine geschützte Maschine mit Exchange Server kann beispielsweise die Optionen „Prüfsummenprüfjob“ und „Exchange-Protokolle kürzen“ enthalten.

5 Klicken Sie auf **OK**.

HINWEIS: Die vorgenommenen Anpassungen gelten jeweils nur für die ausgewählte geschützte Maschine. Um Anpassungen für andere Maschinen durchzuführen, wiederholen Sie die aufgeführten Schritte für jede Maschine, die Sie anpassen möchten. Informationen zum Ändern der Einstellungen für nächtliche Jobs aller durch einen Core geschützten Maschinen finden Sie unter Konfigurieren nächtlicher Jobs für den Core, Konfigurieren von nächtlichen SQL-Anfügbarkeitsprüfungen und Protokollkürzungen für alle geschützten Maschinen oder Konfigurieren von nächtlichen Prüfsummenprüfungen und Protokollkürzungen für Exchange-Datenbanken.

Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion

Wenn Sie den Schutz vorübergehend deaktivieren, werden vorübergehend alle Übertragungen der Daten von der ausgewählten Maschine zum AppAssure Core angehalten. Wenn Sie den Schutz wieder aktivieren, folgt der AppAssure Core dem festgelegten Schutzzeitplan, d. h., die Daten werden dem jeweiligen Zeitplan entsprechend gesichert.

Sie können den Schutz für jede AppAssure Agent-Maschinen vorübergehend deaktivieren:

- Beim Einrichten der Schutzfunktion mit den Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen
- Im Menü „Geschützte Maschinen“ im linken Navigationsbereich des AppAssure Core (Schutz für alle Agenten vorübergehend deaktivieren)
- Auf der Seite „Geschützte Maschinen“ (wird geöffnet, wenn Sie auf das Menü „Geschützte Maschinen“ klicken)
- Im Menü „Geschützte Maschinen“ einer bestimmten geschützten Maschine
- Auf der Registerkarte „Zusammenfassung“ für eine beliebige Agent-Maschine

Wenn Sie den Schutz mit den Assistenten zum Schützen einer Maschine bzw. zum Schützen mehrerer Maschinen vorübergehend deaktivieren, ist der Schutz solange deaktiviert, bis es wieder explizit aktiviert wird.

Wenn Sie den Schutz außerhalb eines Assistenten vorübergehend deaktivieren, können Sie auswählen, ob der Schutz solange deaktiviert werden soll, bis er wieder aktiviert wird, oder die Schutzfunktion für einen bestimmten Zeitraum deaktivieren (Angabe als Kombination von Tagen, Stunden und Minuten). Wenn Sie den Schutz für einen bestimmten Zeitraum deaktivieren, wird die Schutzfunktion nach Ablauf dieses Zeitraums automatisch dem jeweiligen Schutzzeitplan entsprechend wieder aktiviert.

Sie können den Schutz für jeden vorübergehend deaktivierten AppAssure-Agenten wieder aktivieren:

- Im Menü „Geschützte Maschinen“ im linken Navigationsbereich des AppAssure Core (Schutz für alle Agenten wieder aktivieren)
- Im Menü „Geschützte Maschinen“ einer bestimmten geschützten Maschine
- Auf der Seite „Geschützte Maschinen“ (wird geöffnet, wenn Sie auf das Menü „Geschützte Maschinen“ klicken)
- Auf der Registerkarte „Zusammenfassung“ für eine beliebige Agent-Maschine

Gehen Sie folgendermaßen vor, um den Schutz vorübergehend zu deaktivieren bzw. wieder zu aktivieren.

So deaktivieren Sie den Schutz vorübergehend und aktivieren Sie den Schutz wieder

1 Klicken Sie in der AppAssure Core Console auf das Dropdown-Menü **Geschützte Maschinen** im linken Navigationsbereich, um den Schutz für alle Maschinen vorübergehend zu deaktivieren oder wieder zu aktivieren.

- Wenn Sie den Schutz vorübergehend deaktivieren möchten, gehen Sie wie folgt vor:
    a Wählen Sie **Schutz vorübergehend deaktivieren** aus.

      Das Dialogfeld „Schutz vorübergehend deaktivieren“ wird angezeigt.

    b Wählen Sie über die nachstehend beschriebenen Optionen die gewünschte Einstellung aus und klicken Sie auf **OK**.

      - Wählen Sie **Deaktivieren bis Wiederaktivierung**, wenn der Schutz deaktiviert werden soll, bis er wieder aktiviert wird.
      - Wählen Sie **Vorübergehend deaktivieren für (Dauer)** aus, wenn der Schutz für einen bestimmten Zeitraum deaktiviert werden soll, und geben Sie dann über die Steuerelemente Tage, Stunden und Minuten den gewünschten Deaktivierungszeitraum an.

- Wenn Sie den Schutz wieder aktivieren möchten, gehen Sie wie folgt vor:
    a Wählen Sie **Schutz wieder aktivieren** aus.

      Das Dialogfeld „Schutz wieder aktivieren“ wird angezeigt.

    b Klicken Sie im Dialogfeld „Schutz wieder aktivieren“ auf **Ja**.

      Das Dialogfeld „Schutz wieder aktivieren“ wird geschlossen und der Schutz wird für alle Maschinen wieder aktiviert.

2 Um den Schutz für eine einzelne Maschine auf einer Registerkarte vorübergehend zu deaktivieren bzw. wieder zu aktivieren, klicken Sie im linken Navigationsbereich in der Liste der geschützten Maschinen auf den Pfeil rechts neben der betreffenden Maschine.

- Wenn Sie den Schutz vorübergehend deaktivieren möchten, gehen Sie wie folgt vor:
    a Wählen Sie **Schutz vorübergehend deaktivieren** aus.

      Das Dialogfeld „Schutz vorübergehend deaktivieren“ wird angezeigt.

    b Wählen Sie über die nachstehend beschriebenen Optionen die gewünschte Einstellung aus und klicken Sie auf **OK**.

      - Wählen Sie **Deaktivieren bis Wiederaktivierung**, wenn der Schutz deaktiviert werden soll, bis er wieder aktiviert wird.
      - Wählen Sie **Vorübergehend deaktivieren für (Dauer)** aus, wenn der Schutz für einen bestimmten Zeitraum deaktiviert werden soll, und geben Sie dann über die Steuerelemente Tage, Stunden und Minuten den gewünschten Deaktivierungszeitraum an.

- Wenn Sie den Schutz wieder aktivieren möchten, gehen Sie wie folgt vor:
    a Wählen Sie **Schutz wieder aktivieren** aus.

      Das Dialogfeld „Schutz wieder aktivieren“ wird angezeigt.

    b Klicken Sie im Dialogfeld „Schutz wieder aktivieren“ auf **Ja**.

      Das Dialogfeld „Schutz wieder aktivieren“ wird geschlossen und der Schutz wird für die ausgewählte Maschine wieder aktiviert.

3 Um den Schutz für eine einzelne Maschine auf der Registerkarte „Zusammenfassung“ vorübergehend zu deaktivieren bzw. wieder zu aktivieren, navigieren Sie zu der betreffenden Maschine.

  Die Registerkarte „Zusammenfassung“ für die ausgewählte Maschine wird angezeigt.

- Wenn Sie den Schutz vorübergehend deaktivieren möchten, gehen Sie wie folgt vor:
    a Klicken Sie im Dropdown-Menü **Aktionen** für die betreffende Maschine auf **Schutz vorübergehend deaktivieren**.

      Das Dialogfeld „Schutz vorübergehend deaktivieren“ wird angezeigt.

    b Wählen Sie über die nachstehend beschriebenen Optionen die gewünschte Einstellung aus und klicken Sie auf **OK**.

- Wählen Sie **Deaktivieren bis Wiederaktivierung**, wenn der Schutz deaktiviert werden soll, bis er wieder aktiviert wird.
- Wählen Sie **Vorübergehend deaktivieren für (Dauer)** aus, wenn der Schutz für einen bestimmten Zeitraum deaktiviert werden soll, und geben Sie dann über die Steuerelemente Tage, Stunden und Minuten den gewünschten Deaktivierungszeitraum an.

- Wenn Sie den Schutz wieder aktivieren möchten, gehen Sie wie folgt vor:

  a Wählen Sie **Schutz wieder aktivieren** aus.

  Das Dialogfeld „Schutz wieder aktivieren“ wird angezeigt.

  b Klicken Sie im Dialogfeld „Schutz wieder aktivieren“ auf **Ja**.

  Das Dialogfeld „Schutz wieder aktivieren“ wird geschlossen und der Schutz wird für die ausgewählte Maschine wieder aktiviert.

Konfigurieren von Maschineneinstellungen

Sobald Sie Maschinen in AppAssure unter Schutz gestellt haben, können Sie einfach grundlegende Konfigurationseinstellungen für die Maschinen (Name, Hostname usw.), Schutzeinstellungen (Schutzzeitplan für Volumes auf der Maschine ändern, Volumes hinzufügen oder entfernen und/oder den Schutz anhalten) usw. ändern. In diesem Abschnitt werden die verschiedenen Verfahren zum Anzeigen und Ändern von Maschineneinstellungen in AppAssure beschrieben.

Anzeigen und Ändern von Konfigurationseinstellungen

Führen Sie die nachstehend beschriebenen Schritte durch, um Konfigurationseinstellungen zu ändern und anzuzeigen.

Diese Aufgabe ist auch ein Schritt vonÄndern der Einstellungen für Cluster-Knoten.

So zeigen Sie Konfigurationseinstellungen an und ändern Sie Konfigurationseinstellungen

1 Navigieren Sie in der AppAssure Core Console zu der Maschine, für die Sie Konfigurationseinstellungen anzeigen und ändern möchten.

2 Klicken Sie auf die Registerkarte „Konfiguration“.

Die Seite „Einstellungen“ wird angezeigt.

3 Klicken Sie auf **Ändern**, um die in der folgenden Tabelle beschriebenen Maschineneinstellungen zu ändern.

Tabelle 48.

Textfeld	Beschreibung
Anzeigename	Geben Sie einen Anzeigenamen für die Maschine ein. Ein Name für die Maschine, der in der AppAssure Core Console angezeigt werden soll. Standardmäßig ist dies der Hostname für die Maschine. Sie können ihn bei Bedarf in einen aussagekräftigeren Namen ändern.
Hostname	Geben Sie einen Hostnamen für die Maschine ein.
Port	Geben Sie eine Portnummer für die Maschine ein. Der Port wird vom Core für die Kommunikation mit der Maschine genutzt.

Tabelle 48.

Textfeld	Beschreibung
Verschlüsselungs-schlüssel	Bearbeiten Sie ggf. den Verschlüsselungsschlüssel. Geben Sie an, ob die Daten der einzelnen Volumes der Maschine verschlüsselt werden sollen, die im Repository gespeichert werden.
Repository	Wählen Sie ein Repository für die Wiederherstellungspunkte aus. Zeigt das Repository im AppAssure Core an, in dem die Daten für diese Maschine gespeichert werden sollen. **HINWEIS:** Die Einstellung kann nur dann geändert werden, wenn keine Wiederherstellungspunkte vorhanden sind oder das vorherige Repository fehlt.

Anzeigen von Systeminformationen für eine Maschine

Die AppAssure Core Console bietet einfache Zugriffsmöglichkeiten auf alle geschützten Maschinen.

Führen Sie die folgenden Schritte aus, um detaillierte Systeminformationen für eine geschützt Maschine anzuzeigen.

So zeigen Sie die Systeminformationen für eine Maschine an

1. Wählen Sie im linken Navigationsbereich der Core Console unter „Geschützte Maschinen“ die Maschine aus, für die Sie detaillierte Systeminformationen anzeigen möchten.
2. Klicken Sie auf die Registerkarte „Extras“ für die betreffende Maschine. Daraufhin wird die Seite „Systeminformationen“ für die jeweilige Maschine angezeigt.

   Auf der Seite „Systeminformationen“ werden ausführliche Informationen für die jeweilige Maschine angezeigt, z. B.:

   - Hostname
   - Betriebssystem-Version
   - Betriebssystemarchitektur
   - Speicher (Physisch)
   - Anzeigename
   - Vollqualifizierter Domänenname
   - Typ der virtuellen Maschine (sofern zutreffend)

   Darüber hinaus werden detaillierte Informationen zu den Volumes auf dieser Maschine angezeigt, z. B.:

   - Name
   - Geräte-ID
   - Dateisystem
   - Kapazität (einschl. Rohkapazität, formatiert und verwendet)

   Weitere Maschineninformationen, die angezeigt werden, sind:

   - Prozessoren
   - Netzwerkadapter
   - IP-Adressen, die dieser Maschine zugeordnet sind

Konfigurieren von Benachrichtigungsgruppen für Systemereignisse

Sie können in AppAssure konfigurieren, wie Systemereignisse für eine einzelne Maschine gemeldet werden, indem Sie Benachrichtigungsgruppen erstellen. Solche Ereignisse können Systembenachrichtigungen, Fehler usw. sein.

So konfigurieren Sie Benachrichtigungsgruppen für Systemereignisse

1 Navigieren Sie in der AppAssure Core Console zu der Maschine, die Sie ändern möchten.

Die Registerkarte „Zusammenfassung“ wird angezeigt.

2 Klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Ereignisse**.

Die Seite „Benachrichtigungsgruppen“ wird angezeigt.

3 Klicken Sie auf **Benutzerdefinierte Benachrichtigungseinstellungen verwenden**.

Die Anzeige „Benutzerdefinierte Benachrichtigungsgruppen“ wird angezeigt.

4 Klicken Sie auf **Gruppe hinzufügen**, um neue Benachrichtigungsgruppen zum Senden einer Liste der Systemereignisse hinzuzufügen.

Das Dialogfeld „Benachrichtigungsgruppe hinzufügen“ wird angezeigt.

> **HINWEIS:** Um die Standardbenachrichtigungseinstellungen zu verwenden, wählen Sie die Option **Benachrichtigungseinstellungen von Core verwenden** aus.

5 Fügen Sie die in der folgenden Tabelle beschriebenen Benachrichtigungsoptionen hinzu.

Tabelle 49.

Textfeld	Beschreibung
Name	Geben Sie einen Namen für die Benachrichtigungsgruppe ein.
Beschreibung	Geben Sie eine Beschreibung für die Benachrichtigungsgruppe ein.

Tabelle 49.

Textfeld	Beschreibung
Benachrichtigungen aktivieren	Wählen Sie aus, welche Ereignisse Sie für die Benachrichtigungsgruppe freigeben möchten. Sie können **Alle** oder eine Untergruppe von Ereignissen auswählen, z. B.: • Exchange • Autom. Aktualisierung • Deduplizierungscache • Wiederherstellungspunkt-Prüfung • Remote-Bereitstellung • Start-CD • Sicherheit • Datenbankaufbewahrung • Lokale Bereitstellung • Metadaten • Cluster • Benachrichtigung • PowerShell Scripting • Push-Installation • Anfügbarkeit • Jobs • Lizenzierung • Protokollkürzung • Archiv • Core-Dienst • Export • Schutz • Replikation • Repository • Rollback (Wiederherstellung) • Rollup **HINWEIS:** Bei der Auswahl eines bestimmten Typs werden die entsprechenden Ereignisse standardmäßig automatisch aktiviert. Bei Auswahl von *Warnung* werden beispielsweise die folgenden Ereignisse aktiviert: Anfügbarkeit, Jobs, Lizenzierung, Archiv, Core-Dienst, Export, Schutz, Replikation und Rollback (Wiederherstellung).

Tabelle 49.

Textfeld	Beschreibung

Benachrichtigungsoptionen	Wählen Sie die Methode für die Verarbeitung von Benachrichtigungen aus.
	Sie können zwischen folgenden Optionen wählen:
	• **Per E-Mail benachrichtigen**. Sie müssen in den Textfeldern „An“, „CC“ und optional „BCC“ die E-Mail-Adressen angeben, an die die Ereignisse gesendet werden sollen.
	HINWEIS: Um E-Mails erhalten zu können, muss vorher SMTP konfiguriert werden.
	• **Über Windows-Ereignisprotokoll benachrichtigen**. Das Windows-Ereignisprotokoll steuert die Benachrichtigung.
	• **Über syslogd benachrichtigen**. Sie müssen den Hostnamen und Port angeben, an den die Ereignisse gesendet werden sollen.
	  • **Host.** Geben Sie den Hostnamen für den Server ein.
	  • **Port.** Geben Sie eine Portnummer für die Kommunikation mit dem Server ein.
	• **Über Popupbenachrichtigungen benachrichtigen.** Wählen Sie diese Option aus, wenn die Benachrichtigung als Popup in der unteren rechten Ecke des Bildschirms angezeigt werden soll.

6 Klicken Sie auf **OK,** um die Änderungen zu speichern.

7 Um eine vorhandene Benachrichtigungsgruppe zu bearbeiten, klicken Sie auf **Bearbeiten** neben der Benachrichtigungsgruppe, die bearbeitet werden soll**.**

Das Dialogfeld „Benachrichtigungsgruppe bearbeiten“ wird angezeigt, in dem Sie die Einstellungen bearbeiten können.

Bearbeiten von Benachrichtigungsgruppen für Systemereignisse

Führen Sie die folgenden Schritte aus, um Benachrichtigungsgruppen für Systemereignisse zu bearbeiten.

So bearbeiten Sie Benachrichtigungsgruppen für Systemereignisse

1 Navigieren Sie in der AppAssure Core Console zu der Maschine, die Sie ändern möchten.

Die Registerkarte „Zusammenfassung“ wird angezeigt.

2 Klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Ereignisse**.

3 Klicken Sie auf **Benutzerdefinierte Benachrichtigungseinstellungen verwenden**.

Die Anzeige „Benutzerdefinierte Benachrichtigungsgruppen“ wird angezeigt.

4 Klicken Sie auf das Symbol „Bearbeiten“ unter der Spalte „Aktion“.

Das Dialogfeld „Benachrichtigungsgruppe bearbeiten“ wird angezeigt.

5 Bearbeiten Sie die in der folgenden Tabelle beschriebenen Benachrichtigungsoptionen.

Tabelle 50.

Textfeld	Beschreibung
Name	Stellt den Namen der Benachrichtigungsgruppe dar. HINWEIS: Sie können den Namen der Benachrichtigungsgruppe nicht bearbeiten.
Beschreibung	Geben Sie eine Beschreibung für die Benachrichtigungsgruppe ein.

Tabelle 50.

Textfeld	Beschreibung
Benachrichtigungen aktivieren	Wählen Sie aus, welche Ereignisse Sie für die Benachrichtigungsgruppe freigeben möchten. Sie können **Alle** oder eine Untergruppe von Ereignissen auswählen, z. B.: • Exchange • Autom. Aktualisierung • Deduplizierungscache • Wiederherstellungspunkt-Prüfung • Remote-Bereitstellung • Start-CD • Sicherheit • Datenbankaufbewahrung • Lokale Bereitstellung • Metadaten • Cluster • Benachrichtigung • PowerShell Scripting • Push-Installation • Anfügbarkeit • Jobs • Lizenzierung • Protokollkürzung • Archiv • Core-Dienst • Export • Schutz • Replikation • Repository • Rollback (Wiederherstellung) • Rollup Sie können auch den Typ auswählen, z. B.: Info, Warnung und Fehler. **HINWEIS:** Bei der Auswahl eines bestimmten Typs werden die entsprechenden Ereignisse standardmäßig automatisch aktiviert. Bei Auswahl von *Warnung* werden beispielsweise die folgenden Ereignisse aktiviert: Anfügbarkeit, Jobs, Lizenzierung, Archiv, Core-Dienst, Export, Schutz, Replikation und Rollback (Wiederherstellung).

Tabelle 50.

Textfeld	Beschreibung

Benachrichtigungs-optionen	Wählen Sie die Methode für die Verarbeitung von Benachrichtigungen aus. Mögliche Optionen sind:
	• **Per E-Mail benachrichtigen**. Sie müssen in den Textfeldern „An“, „CC“ und optional „BCC“ die E-Mail-Adressen angeben, an die die Ereignisse gesendet werden sollen.
	HINWEIS: Um E-Mails erhalten zu können, muss vorher SMTP konfiguriert werden.
	• **Über Windows-Ereignisprotokoll benachrichtigen**. Das Windows-Ereignisprotokoll steuert die Benachrichtigung.
	• **Über syslogd benachrichtigen**. Sie müssen den Hostnamen und Port angeben, an den die Ereignisse gesendet werden sollen.
	  • **Host.** Geben Sie den Hostnamen für den Server ein.
	  • **Port.** Geben Sie eine Portnummer für die Kommunikation mit dem Server ein.
	• **Über Popupbenachrichtigungen benachrichtigen.** Wählen Sie diese Option aus, wenn die Benachrichtigung als Popup in der unteren rechten Ecke des Bildschirms angezeigt werden soll.

6 Klicken Sie auf **OK**.

Konfigurieren von Standardeinstellungen für die Aufbewahrungsrichtlinie des Core

Die Aufbewahrungsrichtlinie für den Core gibt an, wie lange die Wiederherstellungspunkte für eine Agent-Maschine im Repository gespeichert werden. Die Aufbewahrungsrichtlinie wird durch einen Rollup-Prozess umgesetzt, der im Rahmen der nächtlichen Jobs durchgeführt wird. Wiederherstellungspunkte, die älter sind als das in der Aufwahrungsrichtlinie angegebene Alter werden in weniger Wiederherstellungspunkte zusammengefasst (Rollup), die einen größeren Zeitraum abdecken. Durch die nächtliche Anwendung der Aufbewahrungsrichtlinie erfolgt ein laufender Rollup älterer Sicherungen. Die ältesten Wiederherstellungspunkte werden abhängig von der jeweiligen Aufbewahrungsrichtlinie schließlich gelöscht.

Für Quell- und Ziel-Core können unterschiedliche Aufbewahrungseinstellungen konfiguriert werden.

HINWEIS: In diesem Abschnitt wird die Anpassung der Einstellungen für die Aufbewahrungsrichtlinie auf dem AppAssure Core behandelt. Wenn Sie die angepassten Einstellungen der Aufbewahrungsrichtlinie im Core speichern, werden die Standardeinstellungen für Aufbewahrungsrichtlinien festgelegt, die auf alle Agent-Maschinen angewendet werden können, die durch den jeweiligen Core geschützt werden. Weitere Informationen zum Anpassen der Aufbewahrungsrichtlinieneinstellungen für einzelne Agent-Maschinen finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für einen Agenten.

So konfigurieren Sie die Standardeinstellungen für die Aufbewahrungsrichtlinie des Core

1 Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Aufbewahrungsrichtlinie**.

Die Anzeige „Aufbewahrungsrichtlinie“ mit den Optionen für die Aufbewahrungsrichtlinie des Core wird angezeigt.

2 Geben Sie die primäre Einstellung an. Diese bestimmt, wie lang die anfänglichen Sicherungs-Snapshots aufbewahrt werden. Legen Sie dann die weiteren Rollup-Einstellungen fest, die die Intervalle zwischen den Rollups von Wiederherstellungspunkten bestimmen.

Die Optionen für die Aufbewahrungsrichtlinie werden in der folgenden Tabelle beschrieben.

Tabelle 51.

Textfeld	Beschreibung
Alle Wiederherstellungspunkte beibehalten für (Dauer) *n[Aufbewahrungszeitraum*]	Gibt die Aufbewahrungsdauer für die Wiederherstellungspunkte an. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist *3* Tage. Sie haben folgende Auswahlmöglichkeiten: Tage, Wochen, Monate oder Jahre.
…und anschließend einen Wiederherstellungspunkt pro Stunde beibehalten für *n* [*Aufbewahrungszeitraum*]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird zusammen mit der primären Einstellung verwendet, um die Aufbewahrungsdauer von Wiederherstellungspunkten genauer zu definieren. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist *2* Tage. Sie haben folgende Auswahlmöglichkeiten: Tage, Wochen, Monate oder Jahre.
…und anschließend einen Wiederherstellungspunkt pro Tag beibehalten für *n* [*Aufbewahrungszeitraum*]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird verwendet, um die Aufbewahrungsdauer von Wiederherstellungspunkten genauer zu definieren. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist *4* Tage. Sie haben folgende Auswahlmöglichkeiten: Tage, Wochen, Monate oder Jahre.
…und anschließend einen Wiederherstellungspunkt pro Woche beibehalten für *n* [*Aufbewahrungszeitraum*]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird verwendet, um die Aufbewahrungsdauer von Wiederherstellungspunkten genauer zu definieren. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist *3* Wochen. Sie haben folgende Auswahlmöglichkeiten: Wochen, Monate oder Jahre.
…und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für *n* [*Aufbewahrungszeitraum*]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird verwendet, um die Aufbewahrungsdauer von Wiederherstellungspunkten genauer zu definieren. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist *2* Monate. Sie haben folgende Auswahlmöglichkeiten: Monate oder Jahre.
…und anschließend einen Wiederherstellungspunkt pro Jahr beibehalten für *n* [*Aufbewahrungszeitraum*]	Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Sie haben folgende Auswahlmöglichkeiten: Jahre

Im Textfeld „Neuester Wiederherstellungspunkt“ wird der aktuellste Wiederherstellungspunkt angezeigt. Der älteste Wiederherstellungspunkt wird durch die Einstellungen der Aufbewahrungsrichtlinien bestimmt.

Im folgenden Beispiel wird die Berechnung der Aufbewahrungsdauer veranschaulicht.

Alle Wiederherstellungspunkte beibehalten für *3 Tage*.

...und anschließend einen Wiederherstellungspunkt pro Stunde beibehalten für *3 Tage*

...und anschließend einen Wiederherstellungspunkt pro Tag beibehalten für *4 Tage*

...und anschließend einen Wiederherstellungspunkt pro Woche beibehalten für *3 Wochen*

...und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für *2 Monate*

...und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für *1 Jahr*

Der aktuellste Wiederherstellungspunkt wird auf den aktuellen Tag, den aktuellen Monat und das aktuelle Jahr festgelegt.

In diesem Beispiel wäre der älteste Wiederherstellungspunkt demzufolge 1 Jahr, 4 Monate und 6 Tage alt.

3 Geben Sie unter „Einstellungen“ im Textfeld **Anzahl gleichzeitiger Rollups** einen numerischen Wert ein.

Diese Einstellung bestimmt, wie viele Rollup-Vorgänge gleichzeitig durchgeführt werden können. Wird der Wert auf eine Zahl größer 1 festgelegt, nimmt der Rollup-Prozess weniger Zeit in Anspruch. Die Belastung des Core ist jedoch im Rollup-Zeitraum höher.

HINWEIS: Sie sollten diesen Wert auf 1 einstellen. Falls Rollup-Vorgänge zu lang dauern, können Sie den Wert um 1 erhöhen. Überprüfen Sie anschließend die Systemleistung, um sicherzustellen, dass sich diese Einstellung positiv auf die Umgebung auswirkt.

4 Klicken Sie auf **Übernehmen**.

Die definierte Aufbewahrungsrichtlinie wird im Rahmen der nächtlichen Rollups verwendet.

Sie können diese Einstellungen auch verwendet, wenn Sie die Aufbewahrungsrichtlinie für eine einzelne Agent-Maschine angeben. Weitere Informationen zum Festlegen von Aufbewahrungsrichtlinien für eine Agent-Maschine finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für einen Agenten.

Anpassen der Aufbewahrungsrichtlinieneinstellungen für einen Agenten

Die Aufbewahrungsrichtlinie für eine Agent-Maschine gibt an, wie lange die Wiederherstellungspunkte im Repository gespeichert werden. Sofern Sie keine benutzerdefinierte Aufbewahrungsrichtlinie angeben (siehe folgende Beschreibung), verwendet jeder Agent normalerweise die Standardaufbewahrungsrichtlinie, die für den Core festlegen wurde.

Ab Version 5.4.1 bietet AppAssure 5 die Möglichkeit, unterschiedliche Aufbewahrungsrichtlinien für einen Agenten im Quell-Core und dem entsprechenden replizierten Agenten im Ziel-Core festzulegen.

Gehen Sie folgendermaßen vor, um eine benutzerdefinierte Aufbewahrungsrichtlinie für einen Agenten bzw. einen replizierten Agenten festzulegen.

HINWEIS: Wenn Sie in Umgebungen, bei denen ein Upgrade von AppAssure 5, Release 5.3.x auf Release 5.4.1 oder höher durchgeführt wurde, eine Aufbewahrungsrichtlinie für einen replizierten Agenten anpassen möchten, müssen Sie zuerst Quell- und Ziel-Core auf Release 5.4.1 aktualisieren und anschließend einen Integritätsprüfjob für jedes Repository im betreffenden Ziel-Core durchführen. Die Durchführung dieses Jobs kann abhängig von der Größe des Repositorys und vom zugrunde liegenden Speichersystem erhebliche Zeit in Anspruch nehmen. Informationen zu diesem Job finden Sie unter Informationen zum Integritätsprüfjob für Repositorys. Informationen zur Durchführung dieses Jobs finden Sie unter Ausführen des Integritätsprüfjobs für ein Repository.

Diese Aufgabe ist auch ein Schritt vonÄndern der Einstellungen für Cluster-Knoten.

So passen Sie die Einstellungen von Aufbewahrungsrichtlinien an

1 Navigieren Sie in der AppAssure Core Console zu der Maschine, die Sie ändern möchten.

2 Klicken Sie auf die Registerkarte „Konfiguration“.

Die Seite „Einstellungen“ wird angezeigt.

3 Klicken Sie im Bereich „Nächtliche Jobs“ auf **Ändern**.

Das Dialogfeld „Nächtliche Jobs“ wird angezeigt.

4 Wählen Sie die Option **Rollup** aus, um die gewünschten Zeitintervalle für die Aufbewahrung von Sicherungsdaten anzugeben, und klicken Sie dann auf **Einstellungen**.

Das Konfigurationsdialogfeld für Aufbewahrungsrichtlinien wird angezeigt.

5 Führen Sie den entsprechenden Schritt durch, wenn bei der Anpassung der Aufbewahrungsrichtlinieneinstellungen für einen replizierten Agenten eine Warnung mit dem Hinweis angezeigt wird, dass für das Repository eine Integritätsprüfung durchgeführt werden sollte. Gehen Sie andernfalls zu Schritt 6.

a Klicken Sie auf **Integrität prüfen**, wenn der Job durchgeführt werden kann.

b Klicken Sie auf **Ja**, um den Integritätsprüfjob durchzuführen.

VORSICHT: Die Durchführung kann abhängig von der Größe des Repositorys erhebliche Zeit in Anspruch nehmen. In dieser Zeit können Sie keine anderen Aktionen (Snapshot-Erstellung, Replikation, virtueller Export usw.) im Repository durchführen. Informationen zu diesem Job finden Sie unter Informationen zum Integritätsprüfjob für Repositorys.

- Kehren Sie hierher zurück, nachdem alle untergeordneten Jobs der Integritätsprüfung erfolgreich durchgeführt wurden, und fahren Sie mit dem nächsten Schritt fort.

6 Führen Sie im Konfigurationsdialogfeld eine der folgenden Aktionen aus:

- Wählen Sie die Option **Standard-Aufbewahrungsrichtlinie von Core verwenden** aus, wenn die Standard-Aufbewahrungsrichtlinie für diesen Agenten verwendet werden soll, und klicken Sie dann auf **Speichern**. Die Standardrichtlinie wird auf den betreffenden Agenten angewendet.
- Wählen Sie die Option **Benutzerdefinierte Aufbewahrungsrichtlinie verwenden** aus, wenn Sie eine benutzerdefinierte Aufbewahrungsrichtlinie für den Agenten festlegen möchten, und fahren Sie mit dem nächsten Schritt fort.

7 Geben Sie den benutzerdefinierten Aufbewahrungszeitplan für Wiederherstellungspunkte an (siehe Beschreibung in der folgenden Tabelle).

Tabelle 52.

Textfeld	Beschreibung
Alle Wiederherstellungspunkte beibehalten für (Dauer) *n*[*Aufbewahrungszeitraum*]	Gibt die Aufbewahrungsdauer für die Wiederherstellungspunkte an. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist *3* Tage. Sie haben folgende Auswahlmöglichkeiten: Tage, Wochen, Monate und Jahre.
…und anschließend einen Wiederherstellungspunkt pro Stunde beibehalten für *n* [*Aufbewahrungszeitraum*]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird zusammen mit der primären Einstellung verwendet, um die Aufbewahrungsdauer von Wiederherstellungspunkten genauer zu definieren. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist *2* Tage. Sie haben folgende Auswahlmöglichkeiten: Tage, Wochen, Monate und Jahre.
…und anschließend einen Wiederherstellungspunkt pro Tag beibehalten für *n* [*Aufbewahrungszeitraum*]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird verwendet, um die Aufbewahrungsdauer von Wiederherstellungspunkten genauer zu definieren. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist *4* Tage. Sie haben folgende Auswahlmöglichkeiten: Tage, Wochen, Monate und Jahre.

Tabelle 52.

Textfeld	Beschreibung
…und anschließend einen Wiederherstellungspunkt pro Woche beibehalten für *n* [*Aufbewahrungszeitraum*]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird verwendet, um die Aufbewahrungsdauer von Wiederherstellungspunkten genauer zu definieren. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist *3* Wochen. Sie haben folgende Auswahlmöglichkeiten: Wochen, Monate und Jahre.
…und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für *n* [*Aufbewahrungszeitraum*]	Gibt eine genauere Aufbewahrungsstufe an. Diese Option wird verwendet, um die Aufbewahrungsdauer von Wiederherstellungspunkten genauer zu definieren. Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Die Standardeinstellung ist *2* Monate. Sie haben folgende Auswahlmöglichkeiten: Monate und Jahre.
…und anschließend einen Wiederherstellungspunkt pro Jahr beibehalten für *n* [*Aufbewahrungszeitraum*]	Geben Sie eine Zahl für die Aufbewahrungsdauer an und wählen Sie dann den Zeitraum aus. Sie haben folgende Auswahlmöglichkeiten: Jahre

Im Textfeld „Neuester Wiederherstellungspunkt“ wird der aktuellste Wiederherstellungspunkt angezeigt. Der älteste Wiederherstellungspunkt wird durch die Einstellungen der Aufbewahrungsrichtlinien bestimmt.

Im folgenden Beispiel wird die Berechnung der Aufbewahrungsdauer veranschaulicht.

> Alle Wiederherstellungspunkte beibehalten für *3 Tage*.
>
> ...und anschließend einen Wiederherstellungspunkt pro Stunde beibehalten für *3 Tage*
>
> ...und anschließend einen Wiederherstellungspunkt pro Tag beibehalten für *4 Tage*
>
> ...und anschließend einen Wiederherstellungspunkt pro Woche beibehalten für *3 Wochen*
>
> ...und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für *2 Monate*
>
> ...und anschließend einen Wiederherstellungspunkt pro Monat beibehalten für *1 Jahr*
>
> Der aktuellste Wiederherstellungspunkt wird auf den aktuellen Tag, den aktuellen Monat und das aktuelle Jahr festgelegt.

In diesem Beispiel wäre der älteste Wiederherstellungspunkt demzufolge 1 Jahr, 4 Monate und 6 Tage alt.

8 Klicken Sie auf **Speichern**.

Anzeigen von Lizenzinformationen

Sie können aktuelle Lizenzstatusinformationen für die auf einer Maschine installierte AppAssure Agent-Software anzeigen.

So zeigen Sie Lizenzinformationen an

1 Navigieren Sie in der AppAssure Core Console zu der Maschine, die Sie anzeigen möchten.

2 Klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Lizenzierung**.

Die Statusanzeige wird angezeigt. Sie enthält die folgenden Details zur Produktlizenzierung:

- Ablaufdatum
- Lizenzstatus
- Lizenztyp
- Typ des Agenten

Ändern der Übertragungseinstellungen

In AppAssure können Sie die Einstellungen für die Verwaltung der Datenübertragung für eine geschützte Maschine ändern. Die in diesem Abschnitt beschriebenen Übertragungseinstellungen gelten auf Agentenebene. Informationen zu Übertragungseinstellungen auf Core-Ebene finden Sie unter Ändern der Einstellungen für die Übertragungswarteschlange.

AppAssure unterstützt Windows 8 und Windows Server 2012 für normale Übertragungen (Basisimage und inkrementell) sowie für Wiederherstellung, BMR-Wiederherstellung (Bare Metal Restore) und Export in eine virtuelle Maschine.

Es gibt drei verschieden Übertragungsarten in AppAssure:

- **Snapshot.** Sichert die Daten der geschützten Maschine. Es sind zwei verschiedenartige Snapshots möglich: Basisimage aller geschützten Daten und inkrementelle Snapshots für Daten, die seit dem letzten Snapshot aktualisiert wurden. Bei einer derartigen Übertragung werden Wiederherstellungspunkte erstellt, die im Repository des Core gespeichert werden. Weitere Informationen finden Sie unter Verwalten von Snapshots und Wiederherstellungspunkten.
- **Export in eine virtuelle Maschine.** Erstellt aus einem Wiederherstellungspunkt eine virtuelle Maschine (VM), die alle Daten der Sicherung der geschützten Maschine sowie Betriebssystem und Treiber und zugehörige Daten enthält, damit die VM gestartet werden kann. Weitere Informationen finden Sie unter Information zum Exportieren geschützter Daten von Windows-Maschinen in virtuelle Maschinen.
- **Wiederherstellen**. Stellt die gesicherten Informationen für eine geschützte Maschine wieder her. Weitere Informationen finden Sie unter Wiederherstellen von Volumes aus einem Wiederherstellungspunkt.

  HINWEIS: Bei der Wiederherstellung von Windows-Systemen mit EFI-Systempartitionen wird immer das gesamte Volume zurückgeschrieben.

Bei der Datenübertragung in AppAssure wird ein Daten-Volume über ein Netzwerk von AppAssure Agent-Maschinen zum Core übertragen. Bei einer Replikation werden Daten auch vom Ursprungs- oder Quell-Core zum Ziel-Core übertragen.

Die Datenübertragung kann für das jeweilige System über bestimmte Optionseinstellungen für die Leistung optimiert werden. Diese Einstellungen steuern die genutzte Bandbreite bei der Sicherung von Agent-Maschinen, bei VM-Exportvorgängen bzw. bei einer Wiederherstellung. Die Datenübertragungsleistung wird u. a. durch folgende Faktoren beeinflusst:

- Anzahl der gleichzeitigen Datenübertragungen von Agenten
- Anzahl der gleichzeitigen Datenstreams
- Umfang der geänderten Daten auf den Datenträgern
- Verfügbare Netzwerkbandbreite
- Leistung des Festplattensubsystems d für das Repository
- Verfügbarer Arbeitsspeicher zum Puffern von Daten

Sie können die Leistungsoptionen an die jeweiligen Anforderungen anpassen und die Leitung für die jeweilige Umgebung optimieren.

So ändern Sie die Übertragungseinstellungen

1. Navigieren Sie in der AppAssure Core Console zu der Maschine, die Sie ändern möchten.
2. Klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Übertragungseinstellungen**.

   Die aktuellen Übertragungseinstellungen werden angezeigt.
3. Klicken Sie auf der Seite „Übertragungseinstellungen“ auf **Ändern**.

   Das Dialogfeld „Übertragungseinstellungen“ wird angezeigt.
4. Geben Sie die Optionen für die Übertragungseinstellungen der Maschine ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 53.

Textfeld	Beschreibung
Priorität	Legt die Übertragungspriorität zwischen geschützten Maschinen fest. Sie können damit die Priorität relativ zu anderen geschützten Maschinen zuweisen. Wählen Sie eine Zahl von 1 bis 10 aus. (Dabei ist 1 die höchste Priorität.) Die Standardeinstellung für die Priorität ist 5. **HINWEIS:** Die Priorität wird für Übertragungen verwendet, die sich in der Warteschlange befinden.
Maximale Anzahl gleichzeitiger Streams	Legt die maximale Anzahl von TCP-Verbindungen zum Core fest, die jeweils parallel für einen einzelnen Agenten verarbeitet werden. **HINWEIS:** Dell empfiehlt, diesen Wert auf 8 festzulegen. Vergrößern Sie diese Einstellung, wenn Datenpakete verloren gehen.
Maximale Anzahl gleichzeitiger Schreibvorgänge	Legt die maximale Anzahl gleichzeitiger Festplattenschreibvorgänge für jeweils eine Agentenverbindung fest. **HINWEIS:** Dell empfiehlt, diese Einstellung auf denselben Wert wie für „Maximale Anzahl gleichzeitiger Streams“ festzulegen. Stellen Sie einen geringfügig kleineren Wert ein, wenn Pakete verloren gehen, z. B. auf 7, wenn „Maximale Anzahl gleichzeitiger Streams“ auf 8 festgelegt ist.
Maximale Standardanzahl der Wiederholungen von Core verwenden	Wählen Sie diese Option aus, wenn die Standardanzahl der Wiederholungen für alle geschützten Maschinen verwendet werden soll, falls Vorgänge fehlschlagen.
Maximale Segmentgröße	Gibt die größte Anzahl an Daten (in Byte) an, die ein Computer in einem einzelnen TCP-Segment empfangen kann. Die Standardeinstellung ist 4194304. **VORSICHT: Ändern Sie nicht die Standardeinstellung.**
Maximale Tiefe der Übertragungswarteschlange	Gibt die Anzahl der Befehle an, die gleichzeitig gesendet werden kann. Sie können eine höhere Zahl einstellen, wenn im System eine Vielzahl von gleichzeitigen E/A-Vorgängen durchgeführt wird.
Ausstehende Lesevorgänge pro Stream	Gibt die Anzahl der Lesevorgänge in der Warteschlange an, die im Back-End gespeichert werden. Mit dieser Einstellung können Sie die Warteschlangenverwaltung für Agenten steuern. **HINWEIS:** Dell empfiehlt, diesen Wert auf 24 festzulegen.
Ausgeschlossene Writer	Wählen Sie einen Writer aus, wenn dieser ausgeschlossen werden soll. Da die in der Liste angezeigten Writer spezifisch für die konfigurierte Maschine sind, werden nicht alle Writer in der Liste angezeigt. Die folgenden Writer können u. a. angezeigt werden: • ASR Writer • COM+ REGDB Writer • Performance Counters Writer • Registry Writer • Shadow Copy Optimization Writer • SQLServerWriter • System Writer • Task Scheduler Writer • VSS Metadata Store Writer • WMI Writer
Serverport für Übertragungsdaten	Legt den Port für Übertragungen fest. Die Standardeinstellung ist 8009.

Tabelle 53.

Textfeld	Beschreibung
Zeitüberschreitung für Übertragungen	Gibt den Zeitraum in Minuten und Sekunden an, für den ein Paket ohne Übertragung gleich bleiben darf.
Zeitüberschreitung für Snapshots	Gibt den Zeitraum in Minuten und Sekunden an, für den auf die Erstellung eines Snapshots gewartet wird.
Zeitüberschreitung für Netzwerklesevorgänge	Gibt den Zeitraum in Minuten und Sekunden an, für den auf eine Leseverbindung gewartet wird. Wenn innerhalb dieses Zeitraums kein Netzwerklesevorgang durchgeführt werden kann, wird der Vorgang wiederholt.
Zeitüberschreitung für Netzwerkschreibvorgänge	Gibt die maximale Zeit in Sekunden an, für die auf eine Schreibverbindung gewartet werden soll. Wenn innerhalb dieses Zeitraums kein Netzwerkschreibvorgang durchgeführt werden kann, wird der Vorgang wiederholt.

5 Klicken Sie auf **OK**.

Anzeigen von Systemdiagnoseinformationen

In AppAssure sind Diagnoseinformationen verfügbar, sodass Sie die Protokolldaten einer geschützten Maschine anzeigen können. Darüber hinaus können Sie Diagnoseinformationen für den Core anzeigen und hochladen. Weitere Informationen zum Anzeigen von Maschinenprotokollen finden Sie unter Anzeigen von Maschinenprotokollen. Informationen zum Hochladen von Protokollen finden Sie unter Hochladen von Maschinenprotokollen.

Anzeigen von Maschinenprotokollen

Falls Fehler oder Probleme mit einer Maschine auftreten, kann die Anzeige der Protokolle hilfreich sein.

So zeigen Sie Maschinenprotokolle in der Core Console an

1 Navigieren Sie zur AppAssure Core Console.

2 Klicken Sie auf die Registerkarte „Extras“ und dann auf **Diagnose**.

3 Klicken Sie auf **Protokoll anzeigen**.

Das Dialogfeld „Core-Protokoll herunterladen“ wird angezeigt.

4 Wählen Sie **Klicken Sie hier, um den Download zu starten** aus.

Daraufhin wird eine Meldung mit Informationen zur Datei, die herunterladen wird, und der Frage angezeigt, ob die Datei geöffnet oder gespeichert werden soll.

5 Wählen Sie die gewünschte Methode für die Handhabung der Protokolldatei aus.

So zeigen Sie Maschinenprotokolle einer geschützten Maschine an

1 Navigieren Sie zur AppAssure Core Console, und wählen Sie die Maschine aus, deren Protokolldaten angezeigt werden sollen.

2 Klicken Sie auf die Registerkarte „Extras“ und dann auf **Diagnose**.

3 Klicken Sie auf **Protokoll anzeigen**.

Hochladen von Maschinenprotokollen

Führen Sie die folgenden Schritte aus, um Maschinenprotokolle hochzuladen.

So laden Sie Maschinenprotokolle hoch

1. Navigieren Sie zur AppAssure Core Console.
2. Klicken Sie auf die Registerkarte „Extras“ und dann auf **Diagnose**.
3. Klicken Sie auf **Protokoll hochladen**.

   Das Dialogfeld „Protokoll hochladen“ wird angezeigt.
4. Wählen Sie **Klicken Sie hier, um den Upload zu starten** aus.

   Auf der Registerkarte Ereignisse wird der Status des Uploads der Protokollinformationen für den Core und alle geschützten Maschinen angezeigt.

Verwalten von Core-Jobeinstellungen

Core-Jobs werden automatisch erstellt, wenn Vorgänge eingeleitet werden, z. B. eine Replikation. Im Abschnitt „Jobeinstellungen“ der Registerkarte „Konfiguration“ können Sie die Einstellungen für jeden einzelnen Job festlegen, z. B. die Anzahl der gleichzeitig zulässigen Jobs und die Anzahl der Wiederholungsversuche für einen Job, falls ein Netzwerk- oder Kommunikationsfehler verhindert, dass der Job beim ersten Mal erfolgreich durchgeführt wird.

Bearbeiten von Core-Jobeinstellungen

Führen Sie die folgenden Schritte aus, um die Einstellungen eines Jobs zu bearbeiten.

So bearbeiten Sie Core-Jobeinstellungen

1. Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:
   - Klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Jobeinstellungen**.
   - Klicken Sie auf das Dropdown-Menü der Registerkarte „Konfiguration“ und dann auf **Jobeinstellungen**.
2. Klicken Sie auf der Seite „Jobeinstellungen“ auf **Bearbeiten** für den Job, dessen Einstellungen geändert werden sollen.
3. Das Fenster „Jobeinstellungen [Jobname]“ wird geöffnet.
4. Wählen Sie mit den Aufwärts-/Abwärtspfeilen die Werte für die folgenden Optionen fest:
   - Maximale Anzahl gleichzeitiger Jobs
   - Wiederholungsanzahl
5. Klicken Sie auf **Speichern**.

Hinzufügen von Core-Jobs

Führen Sie die folgenden Schritte aus, um einen Job zum Core hinzuzufügen.

So fügen Sie Core-Jobs hinzu

1. Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:
   - Klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Jobeinstellungen**.

- Klicken Sie auf das Dropdown-Menü der Registerkarte „Konfiguration“ und dann auf **Jobeinstellungen**.

2 Klicken Sie auf der Seite „Jobeinstellungen“ auf **Ändern**.

Das Fenster „Jobeinstellungen“ wird geöffnet.

3 Geben Sie im Fenster „Jobeinstellungen“ die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 54.

Option	Beschreibung
Job	Wählen Sie in der Dropdown-Liste einen der folgenden Jobs aus: • AdHocDeleteRecoveryPointsJob • AutoUpdateJob • BackupJob • BootCdBuilderJob • CheckAgentRecoveryPointsJob • ChecksumCheckJob • CollectDiagnosticInfoJob • DeleteAgentJob • DeleteAllRecveryPointsJob • DeleteAllRecoveryPointsJob • DeleteRecoveryPointsChainJob • DeleteVolumeImagesJob • DownloadExchangeDllsJob • DownloadFromCloudJob • ExportJob • ImportJob • IndexFileDeleteJob • LocalMountRecoveryPointJob • MaintainRepositoryJob • MountabilityCheckJob • NightlyAttachabilityJob • PersistDedupeCacheJob • PushInstallJob • RecoveryPointAttachabilityJob • RollbackJob • RollupJob • UploadCoreLogsJob • UploadExchangeDllsJob • UploadToCloudJob
Maximale Anzahl gleichzeitiger Jobs	Geben Sie die maximale Anzahl von Jobs ein, die gleichzeitig aktiv sein dürfen. **HINWEIS:** Die maximale Anzahl zulässiger Jobs beträgt 50. Der Mindestwert ist 1.
Wiederholungsanzahl	Geben Sie die Anzahl der Wiederholungsversuche des Core ein, den Job durchzuführen.

4 Klicken Sie auf **Speichern**.

Bereitstellen eines Agenten (Push-Installation)

AppAssure bietet die Möglichkeit, den AppAssure Agent Installer auf einzelnen Windows-Maschinen bereitzustellen, die geschützt werden sollen. Führen Sie die folgenden Schritte aus, um das Installationsprogramm mittels Push-Installation auf einem Agenten bereitzustellen.

Informationen zum Bereitstellen von Agenten auf mehreren Maschinen gleichzeitig finden Sie unter Bereitstellung auf mehreren Maschinen.

HINWEIS: Agenten müssen mit einer Sicherheitsrichtlinie konfiguriert sein, die eine Remote-Installation zulässt.

So stellen Sie einen Agenten bereit

1. Klicken Sie in der AppAssure Core Console im linken Navigationsbereich auf „Geschützte Maschinen“, um die Seite „Maschinen“ zu öffnen.
2. Klicken Sie im Dropdown-Menü **Aktionen** auf **Agent bereitstellen**.

   Das Dialogfeld „Agent bereitstellen“ wird angezeigt.
3. Geben Sie im Dialogfeld „Agent bereitstellen“ die in der folgenden Tabelle beschriebenen Anmeldeeinstellungen ein.

   Tabelle 55.

Textfeld	Beschreibung
Maschine	Geben Sie den Hostname oder die IP-Adresse der Maschine ein, die Sie bereitstellen möchten.
Benutzername	Geben Sie den Benutzernamen für die Verbindung zu dieser Maschine ein, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Geben Sie das Kennwort für die Verbindung zu dieser Maschine ein.
Automatischer Neustart nach Installation	Wählen Sie diese Option aus, um anzugeben, ob der Core nach der Bereitstellung und Installation des AppAssure Agent Installers neu gestartet werden soll.

4. Klicken Sie auf **Überprüfen**, um die Anmeldeinformationen zu überprüfen, die Sie eingegeben haben.

   Im Dialogfeld „Agent bereitstellen“ wird eine Meldung mit dem Hinweis angezeigt, dass die Überprüfung durchgeführt wird. Klicken Sie auf **Abbrechen**, um die Überprüfung abzubrechen. Nach Abschluss der Überprüfung wird die Meldung angezeigt, dass die Überprüfung abgeschlossen wurde.
5. Klicken Sie auf **Bereitstellen**.

   Es wird eine Meldung mit dem Hinweis angezeigt, dass die Bereitstellung gestartet wurde. Sie können den Fortschritt auf der Registerkarte „Ereignisse“ verfolgen. Klicken Sie auf **Details anzeigen**, um weitere Informationen zum Status der Agentenbereitstellung anzuzeigen.
6. Klicken Sie auf **OK**.

Verwalten von Maschinen

In diesem Abschnitt werden verschiedene Aufgaben beschrieben, die Sie bei der Verwaltung der Maschinen ausführen können, z. B. Entfernen einer Maschine aus der AppAssure-Umgebung, Einrichten der Replikation, Erzwingen einer Protokollkürzung, Abbrechen von Vorgängen usw.

Entfernen einer Maschine

Führen Sie die folgenden Schritte aus, um den Schutz einer Maschine in der AppAssure-Umgebung aufzuheben.

So entfernen Sie eine Maschine

1. Navigieren Sie in der AppAssure Core Console zu der Maschine, die Sie entfernen möchten.
2. Klicken Sie im Dropdown-Menü **Aktionen** auf **Maschinen entfernen** und wählen Sie dann eine der in der folgenden Tabelle beschriebenen Optionen aus.

   Tabelle 56.

Option	Beschreibung
Wiederherstellungspunkte beibehalten	Alle derzeit gespeicherten Wiederherstellungspunkte für diese Maschine werden beibehalten.
Wiederherstellungspunkte entfernen	Alle derzeit gespeicherten Wiederherstellungspunkte für diese Maschine werden aus dem Repository entfernt.

Abbrechen von Vorgängen für eine Maschine

Sie können aktuell ausgeführte Vorgänge für eine Maschine abbrechen. Dabei können Sie angeben, ob Sie nur die aktuelle Snapshot-Erstellung oder alle aktuellen Vorgänge (z. B. Exportvorgänge, Replikationen usw.) abbrechen möchten.

So brechen Sie Vorgänge für eine Maschine ab

1. Navigieren Sie in der AppAssure Core Console zu der Maschine, für die Sie Vorgänge abbrechen möchten.
2. Klicken Sie auf die Registerkarte „Ereignisse“.
3. Erweitern Sie die Ereignisdetails für das Ereignis oder den Vorgang, den Sie abbrechen möchten.
4. Klicken Sie auf **Abbrechen**.

Anzeigen des Maschinenstatus und anderen Details

Führen Sie die folgenden Schritte aus, um den Status sowie andere Details für eine Maschine anzuzeigen.

So zeigen Sie den Maschinenstatus und andere Details an

- Navigieren Sie in der AppAssure Core Console zu der geschützten Maschine, die Sie anzeigen möchten.

  Die Informationen für die entsprechende Maschine werden auf der Registerkarte „Zusammenfassung“ angezeigt. Die angezeigten Details umfassen:

  - Hostname
  - Letzter erstellter Snapshot
  - Nächster geplanter Snapshot
  - Verschlüsselungsstatus
  - Versionsnummer

  Wenn Exchange Server auf der Maschine installiert ist, werden auch detaillierte Informationen zum Server angezeigt, z. B.:

  - Letzte erfolgreich durchgeführte Bereitstellbarkeitsprüfung
  - Letzte erfolgreich durchgeführte Prüfsummenprüfung
  - Letzte durchgeführte Protokollkürzung

Darüber hinaus werden detaillierte Informationen zu den Volumes auf dieser Maschine angezeigt, z. B.:

- Name
- Dateisystemtyp
- Speicherplatz
- Zeitplan
- Aktueller Zeitplan
- Nächster Snapshot
- Gesamtgröße

Wenn SQL Server auf der Maschine installiert ist, werden auch detaillierte Informationen zum Server angezeigt, z. B.:

- Online-Status
- Name
- Installationspfad
- Version

Wenn Exchange Server auf der Maschine installiert ist, werden auch detaillierte Informationen zum Server und zu den E-Mail-Speichern angezeigt, z. B.:

- Version
- Installationspfad
- Datenpfad
- Datenbankname
- Pfad für Exchange-Datenbanken
- Pfad für Protokolldatei
- Protokollpräfix
- Systempfad
- Mailspeichertyp

Verwalten mehrerer Maschinen

In diesem Abschnitt werden die Aufgaben beschrieben, die Administratoren durchführen müssen, um die AppAssure Agent-Software gleichzeitig auf mehreren Windows-Maschinen bereitzustellen.

Zum Bereitstellen und Schützen mehrerer Agenten müssen Sie die folgenden Aufgaben durchführen:

1 AppAssure auf mehreren Maschinen bereitstellen. Siehe Bereitstellung auf mehreren Maschinen.

2 Aktivität der Batch-Bereitstellung überwachen. Siehe Überprüfen der Bereitstellung auf mehreren Maschinen.

3 Mehrere Maschinen schützen. Siehe Schützen mehrerer Maschinen.

> **HINWEIS:** Dieser Schritt kann übersprungen werden, wenn bei der Bereitstellung die Option **Maschine nach Installation schützen** ausgewählt wurde.

4 Aktivität des Batch-Schutzes überwachen. Siehe Überwachen des Schutzes von mehreren Maschinen.

Bereitstellung auf mehreren Maschinen

Sie können die Bereitstellung der AppAssure Agent-Software auf mehreren Windows-Maschinen mit der Massenbereitstellungsfunktion von Dell AppAssure vereinfachen. In der Core Console können Sie eine Massenbereitstellung auf folgenden Maschinen durchführen:

- Maschinen in einer Active Directory-Domäne
- Maschinen auf einem virtuellen VMware vCenter/ESX(i)-Host
- Maschinen auf beliebigen anderen Hosts

Die Massenbereitstellungsfunktion erkannt Maschinen auf einem Host automatisch und ermöglicht die Auswahl der Maschinen, auf denen die Bereitstellung erfolgen soll. Alternativ können Sie Host- und Maschineninformationen manuell eingeben.

HINWEIS: Mithilfe der Massenbereitstellungsfunktion können Sie die Agent-Software auf bis zu 50 Agent-Maschinen bereitstellen. Die Maschinen, auf denen die Bereitstellung erfolgt, müssen Internetzugang haben, um Software herunterzuladen und zu installieren, da AppAssure die Webversion des AppAssure Agent Installers für die Bereitstellung der Installationskomponenten verwendet. Wenn kein Internetzugang verfügbar ist, müssen Sie den AppAssure Agent Installer manuell vom Dell Software-Lizenzportal herunterladen und auf den Maschinen bereitstellen.

Weitere Informationen finden Sie im *Lizenzportal Benutzerhandbuch* auf der Dokumentationswebsite mit AppAssure-Releaseinformationen und -Handbüchern unter https://support.software.dell.com/appassure/release-notes-guides.

Bereitstellung auf Maschinen in einer Active Directory-Domäne

Um die folgenden Schritte durchführen zu können, benötigen Sie Domäneninformationen und Anmeldeinformationen für den Active Directory-Server.

So führen Sie die Bereitstellung auf mehreren Maschinen in einer Active Directory-Domäne durch

1 Klicken Sie in der AppAssure Core Console auf die Registerkarte „Extras“ und dann auf **Massenbereitstellung**.

2 Klicken Sie im Fenster „Agent auf Maschinen bereitstellen“ auf **Active Directory**.

3 Geben Sie im Dialogfeld „Verbindung mit Active Directory herstellen“ die in der folgenden Tabelle beschriebenen Domänen- und Anmeldeinformationen ein.

Tabelle 57.

Textfeld	Beschreibung
Domäne	Der Hostname oder die IP-Adresse der Active Directory-Domäne.
Benutzername	Der Benutzername für die Verbindung zur Domäne, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Das sichere Kennwort, das für die Verbindung zur Domäne verwendet wird.

4 Klicken Sie auf **Verbinden**.

5 Wählen Sie im Dialogfeld „Maschinen von Active Directory hinzufügen“ die Maschinen aus, auf denen der AppAssure Agent bereitgestellt werden soll, und klicken Sie dann auf **Hinzufügen**.

Die hinzugefügten Maschinen werden im Fenster „Agent auf Maschinen bereitstellen“ angezeigt. Jede hinzugefügte Maschine wird vom System automatisch überprüft.

6 Sie können eine Maschine auch selbst überprüfen, indem Sie die Maschine auswählen und in der Symbolleiste auf **Überprüfen** klicken.

7 Überprüfen Sie anschließend Statussymbol und -meldung für die einzelnen Maschinen auf der Seite „Agent auf Maschinen bereitstellen“. Der Status der Bereitstellbarkeit auf den einzelnen Maschinen wird wie folgt angezeigt:

- Grünes Symbol: AppAssure kann eine Verbindung zur Maschine herstellen und bereitgestellt werden.
- Gelbes Symbol: AppAssure kann eine Verbindung zur Maschine herstellen. Der AppAssure Agent auf der Maschine ist aber bereits mit einem AppAssure Core gepaart.
- Rotes Symbol: AppAssure kann keine Verbindung zur Maschine herstellen. Dies kann daran liegen, dass die Anmeldeinformationen falsch sind, die Maschine ausgeschaltet ist, die Firewall den Datenverkehr blockiert oder ein anderes Problem besteht.

  HINWEIS: Die Agent-Software wird nicht auf Maschinen mit einem roten Statussymbol implementiert.

- Wenn die Statusmeldung für eine Maschine anzeigt, dass die Bereitstellung durchgeführt werden kann, gehen Sie zu Schritt 9.
- Klicken Sie ggf. auf **Details**, wenn die Statusmeldung einen Detail-Link enthält, um festzustellen, ob das Problem korrigiert werden kann.

8 Klicken Sie in der Symbolleiste auf **Einstellungen** oder auf den Link **Bearbeiten** neben der Maschine, um Verbindungsprobleme zu Maschinen mit einem roten Statussymbol zu beheben bzw. den Schutz automatisch zu aktivieren, Port- oder Authentifizierungsinformationen zu ändern, den Anzeigenamen zu ändern, ein Repository anzugeben oder einen Verschlüsselungsschlüssel einzurichten. Gehen Sie dann folgendermaßen vor:

a Geben Sie im Dialogfeld „Einstellungen bearbeiten“ die in der folgenden Tabelle beschriebenen Einstellungen an.

Tabelle 58.

Textfeld	Beschreibung
Hostname	Wird automatisch aus Schritt 3 übernommen.
Benutzername	*Wird automatisch aus Schritt 3 übernommen.*
Kennwort	*Geben Sie das Kennwort für die Maschine ein.*
Automatischer Neustart nach Installation	Obligatorisch. Die Maschine wird nach der Bereitstellung neu gestartet, damit die jeweilige Agent-Maschine geschützt werden kann.
Maschine nach Installation schützen	Diese Option ist standardmäßig ausgewählt. Wenn diese Option ausgewählt ist, wird die Maschine nach der Bereitstellung automatisch geschützt. (Der Schritt Schützen mehrerer Maschinen kann in diesem Fall übersprungen werden.)
Anzeigename	Dieser wird automatisch abhängig vom angegebenen Hostnamen in Schritt 3 zugewiesen. Dieser Name wird in der Core Console für die ausgewählte Maschine angezeigt.
Port	Die Nummer des Ports, über den der AppAssure Core mit dem Agenten auf der Maschine kommuniziert. Die Standardportnummer ist 8006.
Repository	Wählen Sie in der Dropdown-Liste das Repository im AppAssure Core aus, in dem die Daten für die angegebenen Maschinen gespeichert werden sollen. Diese Option ist nur verfügbar, wenn **Maschine nach Installation schützen** ausgewählt wurde.
Verschlüsselungs-schlüssel	(Optional) Wählen Sie über die Dropdown-Liste aus, ob die Daten der angegebenen Maschine verschlüsselt werden sollen. Der Verschlüsselungsschlüssel wird allen geschützten Maschinen zugewiesen. **HINWEIS:** Diese Option ist nur verfügbar, wenn **Maschine nach Installation schützen** ausgewählt wurde.

b Klicken Sie auf **Speichern**.

9 Wählen Sie nach der erfolgreichen Überprüfung der einzelnen Maschinen die Maschinen aus, auf denen der AppAssure Agent bereitgestellt werden soll, und klicken Sie dann auf **Bereitstellen**.

Wenn Sie einen Agenten schützen, der bereits durch einen anderen Core geschützt wird, wird der vorhandene Schutz beendet und die Maschine wird jetzt durch diesen Core geschützt.

Wenn Sie die Option **Maschine nach Installation schützen** auswählen, werden die Maschinen nach einer erfolgreichen Bereitstellung automatisch neu gestartet, sodass der Schutz aktiviert wird.

Bereitstellung auf Maschinen auf einem virtuellen VMware vCenter/ESX(i)-Host

Um die folgenden Schritte durchführen zu können, benötigen Sie Hostinformationen und Anmeldeinformationen für den virtuellen VMware vCenter/ESX(i)-Host.

HINWEIS: Auf allen virtuellen Maschinen müssen die VM Tools installiert sein, da AppAssure den Hostnamen der virtuellen Maschine nicht ermitteln kann, auf dem die Bereitstellung erfolgen soll. Anstelle des Hostnamens verwendet AppAssure den Namen der virtuellen Maschine. Dies kann zu Problemen führen, wenn der Hostname mit dem Namen der virtuellen Maschine übereinstimmt.

So führen Sie die Bereitstellung auf einem virtuellen VMware vCenter/ESX(i)-Host durch

1 Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Extras“ und dann auf **Massenbereitstellung**.

2 Klicken Sie im Fenster „Agent auf Maschinen bereitstellen“ auf **vCenter/ESX(i)**.

3 Geben Sie im Dialogfeld „Verbindung mit vCenter Server/ESX(i) herstellen“ die nachstehend aufgeführten Host- und Anmeldeinformationen ein und klicken Sie auf **Verbinden**.

Tabelle 59.

Textfeld	Beschreibung
Host	Der Hostname oder die IP-Adresse des virtuellen VMware vCenter/ESX(i)-Hosts.
Port	Der Port für die Verbindung zum virtuellen Host. Die Standardeinstellung ist 443.
Benutzername	Der Benutzername für die Verbindung zum virtuellen Host, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Das sichere Kennwort, das für die Verbindung zum jeweiligen virtuellen Host verwendet wird.

4 Gehen Sie im Dialogfeld „Maschinen von VMware vCenter Server/ESX(i) hinzufügen“ folgendermaßen vor:

a Geben Sie unter „Optionen“ den Benutzernamen und das Kennwort für die ausgewählten virtuellen Maschinen ein.

b Klicken Sie auf die Pfeile neben den einzelnen Knoten, um die Maschinen zu durchsuchen, indem Sie Cluster, Ressourcenpools, vApps und virtuelle Maschinen erweitern oder reduzieren.

c Wählen Sie die Maschinen aus, auf denen die Bereitstellung durchgeführt werden soll, und klicken Sie dann auf **Hinzufügen**.

Die hinzugefügten Maschinen werden im Fenster „Agent auf Maschinen bereitstellen“ angezeigt. Jede hinzugefügte Maschine wird vom System automatisch überprüft.

5 Optional können Sie Maschinen überprüfen, den Status von Maschinen ermitteln oder Verbindungseinstellungen für eine Maschine bearbeiten (siehe Beschreibung in Schritt 6 bis Schritt 8 unter Bereitstellung auf Maschinen in einer Active Directory-Domäne).

6 Aktivieren Sie nach der erfolgreichen Überprüfung der Maschinen das Kontrollkästchen neben den Maschinen, auf denen der AppAssure Agent bereitgestellt werden soll, und klicken Sie dann auf **Bereitstellen**.

Wenn Sie einen Agenten schützen, der bereits durch einen anderen Core geschützt wird, wird der vorhandene Schutz beendet und die Maschine wird jetzt durch diesen Core geschützt.

Wenn Sie die Option **Maschine nach Installation schützen** auswählen, werden die Maschinen nach einer erfolgreichen Bereitstellung automatisch neu gestartet, sodass der Schutz aktiviert wird.

Bereitstellung auf Maschinen auf beliebigen anderen Hosts

So führen Sie die Bereitstellung auf mehreren Maschinen auf beliebigen anderen Hosts durch

1 Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Extras“ und dann auf **Massenbereitstellung**.

2 Führen Sie im Fenster „Agent auf Maschinen bereitstellen“ eine der folgenden Aktionen durch:

- Klicken Sie auf **Neu**, und geben Sie einen neuen Maschinenhost, Anmeldeinformationen, Anzeigenamen (optional), Repository, Verschlüsselungsschlüssel und weitere Informationen eine. Details zu den einzelnen Einstellungen finden Sie unter Bereitstellung auf Maschinen in einer Active Directory-Domäne.

  Klicken Sie auf **OK**, nachdem Sie diese Informationen eingegeben haben, um sie zur Liste „Agent auf Maschinen bereitstellen“ hinzuzufügen, oder klicken Sie auf **OK & Neu**, um eine weitere Maschine hinzuzufügen.

  > **HINWEIS:** Aktivieren Sie das Kontrollkästchen **Maschine nach Installation schützen**, wenn die Maschine nach der Bereitstellung automatisch geschützt werden soll. Wenn Sie das Kontrollkästchen aktivieren, wird die Maschine automatisch neu gestartet, um den Schutz zu aktivieren.

- Um mehrere Maschinen in einer Liste anzugeben, klicken Sie auf **Manuell**. Gaben Sie anschließend die Maschinendetails im Dialogfeld „Maschinen manuell hinzufügen“ ein und klicken Sie auf **Hinzufügen**. Für jede Maschine müssen Sie die IP-Adresse oder den Namen der Maschine, den Benutzernamen, das Kennwort und den Port, jeweils getrennt durch einen doppelten Doppelpunkt im folgenden Format eingeben:

  ```
  Hostname::Benutzername::Kennwort::Port
  ```

  Beispiel:

  ```
  10.255.255.255::administrator::&11@yYz90z::8006
  ```

  ```
  abc-host-00-1::administrator::99!zU$o83r::168
  ```

Die hinzugefügten Maschinen werden im Fenster „Agent auf Maschinen bereitstellen“ angezeigt. Jede hinzugefügte Maschine wird vom System automatisch überprüft.

3 Optional können Sie Maschinen überprüfen, den Status von Maschinen ermitteln oder Verbindungseinstellungen für eine Maschine bearbeiten (siehe Beschreibung in Schritt 6 bis Schritt 8 unter Bereitstellung auf Maschinen in einer Active Directory-Domäne).

4 Aktivieren Sie nach der erfolgreichen Überprüfung der Maschinen das Kontrollkästchen neben den Maschinen, auf denen der AppAssure Agent bereitgestellt werden soll, und klicken Sie dann auf **Bereitstellen**.

Wenn Sie einen Agenten schützen, der bereits durch einen anderen Core geschützt wird, wird der vorhandene Schutz beendet und die Maschine wird jetzt durch diesen Core geschützt.

Wenn Sie die Option **Maschine nach Installation schützen** auswählen, werden die Maschinen nach einer erfolgreichen Bereitstellung automatisch neu gestartet, sodass der Schutz aktiviert wird.

Überprüfen der Bereitstellung auf mehreren Maschinen

Nach der Massenbereitstellung der AppAssure Agent-Software auf mehreren Maschinen können Sie überprüfen, ob die Bereitstellung erfolgreich war, indem Sie die einzelnen Maschinen in der Liste unter dem Menü „Geschützte Maschinen“ anzeigen.

Sie können die Informationen zur Massenbereitstellung auch auf der Registerkarte „Ereignisse“ sehen. Führen Sie die folgenden Schritte aus, um die Bereitstellung zu überprüfen.

So überprüfen Sie die Bereitstellung auf mehreren Maschinen

1. Navigieren Sie zur AppAssure Core Console, klicken Sie auf die Registerkarte „Ereignisse“ und dann auf **Benachrichtigungen**.
2. Navigieren Sie zur Registerkarte „Startseite“ des AppAssure Core und klicken Sie auf die Registerkarte **Ereignisse**.

   In der Liste werden die Benachrichtigungsereignisse mit der Uhrzeit, zu der das Ereignis aufgetreten ist, und eine zugehörige Meldung angezeigt. Für jede erfolgreiche Bereitstellung der Agent-Software wird eine Benachrichtigung angezeigt, dass die geschützte Maschine hinzugefügt wurde.
3. Sie können auf jeden Link für eine geschützte Maschine klicken.

   Die Registerkarte „Zusammenfassung“ für die ausgewählte Maschine wird mit Informationen zur jeweiligen Maschine angezeigt, z. B.:

   - Hostame der geschützten Maschine
   - Letzter Snapshot (sofern zutreffend)
   - Planmäßiger Zeitpunkt der nächsten Snapshot-Erstellung gemäß Schutzzeitplan, der ausgewählt wurde
   - Verschlüsselungsschlüssel (sofern vorhanden) für den jeweiligen geschützten Agenten
   - Version der Agent-Software

Schützen mehrerer Maschinen

Mit dem Assistenten zum Schützen mehrerer Maschinen können Sie zwei oder mehr Windows-Maschinen gleichzeitig dem Schutz durch den AppAssure Core unterstellen. Diese Funktion wird Massenschutz genannt.

Wie beim Schützen einzelner Agent-Maschinen muss die AppAssure Agent-Software beim Massenschutz auf jeder Maschine installiert werden, die geschützt werden soll. Ebenso müssen die Maschinen nach der Installation der Agent-Software neu gestartet werden. Es gibt mehrere Möglichkeiten, die Agent-Software gleichzeitig auf mehreren Maschinen bereitzustellen. Beispiel:

- Sie können die Agent-Software mithilfe der Massenbereitstellungsfunktion auf der Registerkarte „Extras“ auf mehreren Maschinen installieren. (Sie können diesen Schritt überspringen, wenn Sie bei der Bereitstellung des Agenten die Option **Maschine nach Installation schützen** ausgewählt haben.) Weitere Informationen zur Massenbereitstellungsfunktion finden Sie unter Bereitstellung auf mehreren Maschinen.
- Sie können die Agent-Software mit diesem Assistenten installieren.

HINWEIS: Die Agent-Maschinen müssen mit einer Sicherheitsrichtlinie konfiguriert sein, die eine Remote-Installation zulässt.

Der Workflow des Assistenten zum Schützen mehrerer Maschinen kann abhängig von der jeweiligen Umgebung geringfügig abweichen. Wenn beispielsweise die Agent-Software auf den zu schützenden Maschinen installiert ist, werden Sie im Assistenten nicht aufgefordert, die Software zu installieren. Ebenso werden Sie nicht aufgefordert, ein Repository zu erstellen, wenn im Core bereits ein Repository vorhanden ist.

Diese Vorgehensweise umfasst optionale Schritte, die Sie durchführen können, wenn Sie eine erweiterte Konfiguration auswählen. Dies umfasst Repository-Funktionen. (Sie können ein vorhandenes AppAssure-Repository zum Speichern von Snapshots angeben oder ein neues Repository erstellen.) Sie können die Daten der jeweiligen Maschine, die im Core gespeichert werden, auch verschlüsseln.

So schützen Sie mehrere Maschinen

1 Starten Sie die Maschinen neu, wenn die AppAssure Agent-Software auf den zu schützenden Maschinen bereits installiert, die Maschinen aber noch nicht neu gestartet wurden.

2 Navigieren Sie auf der Core-Maschine zur AppAssure Core Console, klicken Sie auf das Dropdown-Menü neben dem Symbol „Schützen“ und wählen Sie **Massenschutz** aus.

Der Assistent zum Schützen mehrerer Maschinen wird angezeigt.

3 Wählen Sie auf der Begrüßungsseite die gewünschten Installationsoptionen aus:

- Wählen Sie **Standard** aus, wenn Sie kein Repository definieren und keine Verschlüsselung einrichten müssen.
- Wählen Sie **Erweitert (optionale Schritte anzeigen)** aus, wenn Sie ein Repository erstellen, ein anderes Repository für Sicherungen der ausgewählten Maschinen angeben oder die Verschlüsselung mit dem Assistenten einrichten müssen.
- Sie können die Option **Diese Begrüßungsseite beim nächsten Start des Assistenten überspringen** auswählen, wenn die Begrüßungsseite des Assistenten zum Schützen einer Maschine nicht mehr angezeigt werden soll.

4 Wenn Sie die gewünschten Optionen auf der Begrüßungsseite festgelegt haben, klicken Sie auf **Weiter**.

Die Seite „Verbindung“ wird angezeigt.

5 Wählen Sie die entsprechende Methode zum Ermitteln der Maschinen aus, die unter Schutz gestellt werden sollen.

Die Maschinen müssen eingeschaltet und zugänglich sein, damit eine Verbindung hergestellt werden kann. Damit für Massenschutz und Massenbereitstellung eine erfolgreiche Verbindung mit Active Directory hergestellt werden kann, sollten Sie sich bei den Maschinen als Domänenadministrator anmelden.

- Wenn die Maschinen in einer Active Directory-Domäne geschützt werden sollen, wählen Sie **Verbindung mit Active Directory herstellen** aus, geben Sie die in der folgenden Tabelle beschriebenen Anmeldeinformationen ein und klicken Sie dann auf **Weiter**. Gehen Sie zu Schritt 7.
- Wenn die Maschinen auf einem virtuellen VMware vCenter/ESX(i)-Host geschützt werden sollen, wählen Sie **Verbindung zu vCenter/ESX(i) herstellen** aus, geben Sie die in der folgenden Tabelle beschriebenen Anmeldeinformationen ein und klicken Sie dann auf **Weiter**. Gehen Sie zu Schritt 7.

Tabelle 60.

Textfeld	Beschreibung
Host	Der Hostname oder die IP-Adresse der Active Directory-Domäne oder des virtuellen VMware vCenter/ESX(i)-Hosts.
Benutzername	Der Benutzername für die Verbindung zur Domäne, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).
Kennwort	Das sichere Kennwort, das für die Verbindung zur Domäne verwendet wird.

HINWEIS: Auf allen virtuellen Maschinen müssen die VM Tools installiert sein, da AppAssure den Hostnamen der virtuellen Maschine nicht ermitteln kann, auf dem die Agent-Software bereitgestellt wird, und die betreffende Maschine nicht geschützt werden kann. Anstelle des Hostnamens verwendet AppAssure den Namen der virtuellen Maschine. Dies kann zu Problemen führen, wenn der Hostname mit dem Namen der virtuellen Maschine übereinstimmt.

- Wählen Sie **Maschinen manuell hinzufügen** aus, wenn die Maschinen manuell hinzugefügt werden sollen, und klicken Sie auf **Weiter**.

Die Seite „Maschinen“ wird angezeigt.

6 Geben Sie auf der Seite „Maschinen“ die Verbindungsdetails der einzelnen Maschinen in einer separaten Zeile ein, um die Maschinen manuell anzugeben, und klicken Sie dann auf **Weiter**. Verwenden Sie das folgende Format:

```
Hostname::Benutzername::Kennwort::Port
```

> **HINWEIS:** Der Port-Parameter ist optional; ohne Angabe wird standardmäßig Port 8006 verwendet. Wenn Sie einen anderen Port als 8006 angeben möchten, müssen Sie diesen Parameter explizit angeben.

7 Wählen Sie auf der Seite „Maschinen“ die einzelnen Maschinen, die geschützt werden sollen, in der Liste aus, um die Maschinen einer Active Directory-Domäne oder eines virtuellen VMware vCenter/ESX(i)-Hosts anzugeben. Achten Sie darauf, dass die Kontrollkästchenoption für alle Maschinen, die derzeit nicht geschützt werden sollen, deaktiviert ist. Klicken Sie auf **Weiter**, wenn die Angaben in Ordnung sind.

Jede hinzugefügte Maschine wird vom System automatisch überprüft.

8 Wechseln Sie zu Schritt 12, wenn als Nächstes die Seite „Schutz“ im Assistenten angezeigt wird.

Wenn die Agent-Software noch nicht auf den zu schützenden Maschinen bereitgestellt wurde oder eine Maschine aus einem anderen Grund nicht geschützt werden kann, werden die ausgewählten Maschinen auf einer entsprechenden Warnseite angezeigt. Jede hinzugefügte Maschine wird vom System automatisch überprüft.

9 Sie können eine Maschine auf der Warnseite für Maschinen auch selbst überprüfen, indem Sie die Maschine auswählen und in der Symbolleiste auf **Überprüfen** klicken.

10 Wählen Sie auf der Warnseite für Maschinen ggf. **Maschinen nach der Agent-Installation automatisch neu starten** aus.

> **HINWEIS:** Dell empfiehlt, diese Option auszuwählen. Sie müssen die Agent-Maschinen neu starten, damit sie geschützt werden können.

11 Klicken Sie auf **Weiter**, wenn der Status anzeigt, dass die Maschine erreichbar ist, um die Agent-Software zu installieren.

Die Seite „Schutz“ wird angezeigt.

12 Wählen Sie auf der Seite „Schutz“ den gewünschten Schutzzeitplan aus (siehe nachstehende Beschreibung).

- Wählen Sie unter „Zeitplaneinstellungen“ die Option **Standardschutz (stündliche Snapshots aller Volumes)** aus, um den Standardschutzzeitplan zu verwenden.
- Wählen Sie unter „Zeitplaneinstellungen“ die Option **Benutzerdefinierter Schutz** aus, um einen anderen Schutzzeitplan zu definieren, und klicken Sie auf **Weiter**.

13 Setzen Sie die Konfiguration wie folgt fort:

- Klicken Sie auf **Fertigstellen**, wenn Sie im Assistenten die Standardkonfiguration und Standardschutz ausgewählt haben, um die ausgewählten Einstellungen zu bestätigen, den Assistenten zu schließen und die angegebenen Maschinen zu schützen.
- Klicken Sie auf der Seite „Schutz“ auf **Weiter**, wenn Sie im Assistenten die Standardkonfiguration und benutzerdefinierten Schutz ausgewählt haben. Richten Sie anschließend auf der Seite Schutzzeitplan einen benutzerdefinierten Zeitplan ein (siehe Beschreibung unter Erstellen benutzerdefinierter Schutzzeitpläne). Klicken Sie dann auf **Fertigstellen**, um die ausgewählten Optionen zu bestätigen, den Assistenten zu schließen und die angegebenen Maschinen zu schützen.
- Klicken Sie auf **Weiter**, wenn Sie im Assistenten die erweiterte Konfiguration ausgewählt haben, und gehen Sie zu Schritt Schritt 14, um Repository- und Verschlüsselungsoptionen anzugeben.

14 Wählen Sie auf der Seite „Repository“ **Vorhandenes Repository verwenden** aus, wenn die zu schützenden Daten aller angegebenen Maschinen in einem vorhandenen Repository gespeichert werden sollen. Wählen Sie das entsprechende Repository in der Liste aus, klicken Sie auf **Weiter** und fahren Sie mit Schritt 19 fort.

Gehen Sie folgendermaßen vor, um einen neuen Speicherort im Core zu erstellen:

a Wählen Sie **Repository erstellen** aus.

b Geben Sie auf der Seite „Repository“ im Feld **Name** den Namen des Repositorys an, das Sie erstellen möchten.

Das Feld enthält normalerweise das Wort „Repository“ sowie eine Indexnummer, die der Nummer des neuen Repositorys entspricht (z. B. **Repository1**). Sie können den Namen bei Bedarf ändern. Sie können bis zu 40 Zeichen eingeben. Der Name muss für den Core eindeutig sein.

HINWEIS: Verwenden Sie im Repositorynamen nur alphanumerische Zeichen und Bindestriche. Andere Symbole oder Interpunktionszeichen sind nicht zulässig. Verwenden Sie keine Buchstabenkombinationen, die mit Befehlen oder reservierten Wörtern übereinstimmen (z. B. con, prn, aux oder nul) oder Anschlüsse darstellen (z. B. com oder lpt).

c Geben Sie im **Speicherort** einen Verzeichnispfad für das Repository ein. Geben Sie beispielsweise für ein Repository auf einem lokalen Computer **C:\Repository** ein. Der Speicherort muss für den Core eindeutig sein. Geben Sie das Repository im Format \\Servername\Freigabename an, wenn das Repository in einem freigegebenen Laufwerk gespeichert werden soll.

VORSICHT: Wenn Sie das Repository später löschen, entfernt das Installationsprogramm alle Inhalte im Repositorypfad. Erstellen Sie den Speicherort deshalb nicht im Stammverzeichnis (z. B. c:\), da dann alle auf dem betreffenden Volume gespeicherten Daten verloren gehen können.

d Geben Sie im Feld **Benutzername** einen Benutzernamen mit Zugriffsberechtigungen für das freigegeben Laufwerk und im Feld **Kennwort** das Kennwort für diesen Benutzer ein, wenn das Repository auf einem freigegebenen Volume gespeichert wird.

e Geben Sie im Feld **Metadatenpfad** den Pfad ein, in dem Metadaten gespeichert werden sollen. Dies sollte in Unterverzeichnis des Speicherorts sein. Geben Sie beispielsweise **C:\Repository\Metadata** ein, wenn C:\Repository als Speicherort angegeben wurde. Der Pfad muss für den Core eindeutig sein.

15 Klicken Sie auf **Weiter**, wenn Sie alle erforderlichen Daten auf der Seite „Repository“ angegeben haben.

Die Seite „Repository-Konfiguration“ wird angezeigt.

16 Geben Sie die Größe des Repositorys ein.

HINWEIS: Wenn es sich beim Speicherort um ein NTFS-Volume (New Technology File System) unter Windows XP oder Windows 7 handelt, ist die Dateigröße auf 16 TB beschränkt.

Wenn es sich beim Speicherort um ein NTFS-Volume (New Technology File System) unter Windows 8, 8.1 oder Windows Server 2012, 2012 R2 handelt, ist die Dateigröße auf 256 TB beschränkt.

Damit AppAssure das Betriebssystem überprüfen kann, muss die Windows-Verwaltungsinstrumentation (WMI) auf dem beabsichtigten Speicherort installiert sein.

17 Wählen Sie **Erweiterte Optionen anzeigen** aus, um die Bytes pro Sektor oder die Bytes pro Datensatz anzugeben bzw. die Schreib-Caching-Richtlinie festzulegen, und geben Sie dann die in der folgenden Tabelle beschriebenen Details für den Speicherort ein.

Tabelle 61.

Textfeld	Beschreibung
Bytes pro Sektor	Geben Sie die Anzahl an Bytes an, die jeder Sektor enthalten soll. Der Standardwert ist *512*.

Tabelle 61.

Textfeld	Beschreibung
Bytes pro Datensatz	Geben Sie die durchschnittliche Anzahl an Bytes pro Datensatz an. Der Standardwert ist *8192*.
Schreib-Caching-Richtlinie	Die Schreib-Caching-Richtlinie steuert, wie der Windows Cache-Manager im Repository verwendet wird. Sie ermöglicht die Optimierung der Repository-Leistung bei unterschiedlichen Konfigurationen. Legen Sie den Wert auf eine der folgenden Optionen fest: • Ein • Aus • Sync Bei Auswahl der Standardeinstellung *Ein* steuert Windows das Caching. **HINWEIS:** Wenn die Schreib-Caching-Richtlinie auf *Ein* festgelegt wird, kann die Leistung gesteigert werden. Wenn Sie eine Version von Windows Server vor Server 2012, ist die empfohlene Einstellung *Aus*. Bei Auswahl von *Aus* steuert AppAssure das Caching. Bei Auswahl von *Sync* steuert Windows das Caching sowie die synchrone Eingabe/Ausgabe.

18 Wenn Sie die gewünschten Informationen für die Repositorykonfiguration eingegeben haben, klicken Sie auf **Weiter**.

Die Seite „Verschlüsselung“ wird angezeigt.

19 Wählen Sie ggf. auf der Seite „Verschlüsselung“ die Option **Verschlüsselung aktivieren** aus, um die Verschlüsselung zu aktivieren.

Daraufhin werden auf der Seite „Verschlüsselung“ Felder für Verschlüsselungsschlüssel angezeigt.

HINWEIS: Wenn Sie die Verschlüsselung aktivieren, werden die Daten aller geschützten Volumes für alle zu schützenden Maschinen verschlüsselt. Sie können die Einstellungen später auf der Registerkarte „Konfiguration“ in der AppAssure Core Console ändern. Weitere Informationen zur Verschlüsselung finden Sie unter Verwalten der Sicherheit.

VORSICHT: AppAssure verwendet 256-Bit-AES-Verschlüsselung im CBC-Modus (Cipher Block Chaining) mit 256-Bit-Schlüsseln. Obwohl die Verwendung der Verschlüsselung optional ist, wird von Dell dringend empfohlen, einen Verschlüsselungsschlüssel einzurichten und die festgelegte Passphrase zu schützen. Speichern Sie die Passphrase an einem sicheren Speicherort, da sie für die Datenwiederherstellung von entscheidender Bedeutung ist. Ohne Passphrase ist keine Datenwiederherstellung möglich.

20 Geben Sie die in der folgenden Tabelle beschriebenen Informationen ein, um einen Verschlüsselungsschlüssel für den Core hinzuzufügen.

Tabelle 62.

Textfeld	Beschreibung
Name	Geben Sie einen Namen für den Verschlüsselungsschlüssel ein.
Beschreibung	Geben Sie eine Beschreibung mit weiteren Details für den Verschlüsselungsschlüssel ein.
Passphrase	Geben Sie die Passphrase für die Zugriffssteuerung ein.
Passphrase wiederholen	Geben Sie zuvor eingegebene Passphrase erneut ein.

21 Klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern und zu übernehmen.

Der Assistent wird geschlossen. Die Agent-Software wird auf den angegebenen Maschinen (sofern erforderlich) und die Maschinen werden unter Schutz durch den Core gestellt.

Überwachen des Schutzes von mehreren Maschinen

Sie können den Fortschritt überwachen, während AppAssure die Schutzrichtlinien und Zeitpläne auf die Maschinen anwendet.

So überwachen Sie den Schutz von mehreren Maschinen

- Navigieren Sie in der AppAssure Core Console zur AppAssure-Registerkarte **Startseite** und klicken Sie auf die Registerkarte **Ereignisse**.

  Auf der Registerkarte „Ereignisse“ werden Aufgaben, Benachrichtigungen und Ereignisse angezeigt. Wenn Volumes übertragen werden, werden im Fensterbereich „Aufgaben“ der jeweilige Status sowie Start- und Endzeiten angezeigt.

  Sie können Aufgaben auch nach Status filtern (Aktiv, System wartet, Abgeschlossen und Fehlgeschlagen). Weitere Informationen finden Sie unter Anzeigen von Aufgaben.

  HINWEIS: Damit nur Aufgaben angezeigt werden, die auf ihre Ausführung warten, müssen Sie das Symbol für wartende Aufgaben auswählen.

  Beim Hinzufügen der einzelnen geschützten Maschinen wird eine Benachrichtigung protokolliert, die angibt, ob der Vorgang erfolgreich war oder ob Fehler gemeldet wurden. Weitere Informationen finden Sie unter Anzeigen von Benachrichtigungen.

  Informationen zum Anzeigen aller Ereignisse finden Sie unter Anzeigen aller Ereignisse.

Verwalten von Snapshots und Wiederherstellungspunkten

Bei einem Wiederherstellungspunkt handelt es sich um eine Gruppe von Snapshots der einzelnen Datenträger-Volumes, die im Repository gespeichert sind. Snapshots erfassen und speichern den Zustand eines Datenträger-Volumes zu einem bestimmten Zeitpunkt, während die Anwendungen, die die Daten generieren, genutzt werden. In AppAssure können Sie einen Snapshot erzwingen, Snapshots vorübergehend deaktivieren, Listen mit aktuellen Wiederherstellungspunkten im Repository anzeigen und diese bei Bedarf löschen. Wiederherstellungspunkte werden für die Wiederherstellung geschützter Maschinen oder für die Bereitstellung in einem lokalen Dateisystem verwendet.

Die von AppAssure erfassten Snapshots werden auf Blockebene erstellt und sind anwendungskonsistent. Das heißt, dass alle offenen Transaktionen und laufenden Transaktionsprotokolle abgeschlossen und die Cache-Speicher auf der Festplatte abgelegt werden, bevor der Snapshot erstellt wird.

AppAssure verwendet einen hardwarenahen Volume-Filtertreiber, der den bereitgestellten Volumes zugeordnet wird und alle Änderungen auf Blockebene für den nächsten bevorstehenden Snapshot protokolliert. Mithilfe der Microsoft Volumeschattenkopie-Dienste (VSS) werden anwendungs- und absturzkonsistente Snapshots ermöglicht.

Anzeigen von Wiederherstellungspunkten

Führen Sie die folgenden Schritte aus, um Wiederherstellungspunkte anzuzeigen.

So zeigen Sie Wiederherstellungspunkte an

1. Navigieren Sie in der AppAssure Core Console zu der geschützten Maschine, für die Sie Wiederherstellungspunkte anzeigen möchten.
2. Klicken Sie auf die Registerkarte „Wiederherstellungspunkte“.

   Sie können die in der folgenden Tabelle beschriebenen Informationen für die Wiederherstellungspunkte der Maschine anzeigen.

Tabelle 63.

Info	Beschreibung
Status	Zeigt den aktuellen Status des Wiederherstellungspunkts an.
Verschlüsselt	Zeigt an, ob der Wiederherstellungspunkt verschlüsselt ist.
Inhalt	Zeigt eine Liste der im Wiederherstellungspunkt enthaltenen Volumes an.
Typ	Gibt an, ob der Wiederherstellungspunkt ein Basisimage oder ein inkrementeller (differenzieller) Snapshot ist.
Erstellungsdatum	Zeigt das Datum an, an dem der Wiederherstellungspunkt erstellt wurde.
Größe	Zeigt den Speicherplatz an, den der Wiederherstellungspunkt im Repository belegt.

Anzeigen eines bestimmten Wiederherstellungspunkts

Führen Sie die folgenden Schritte aus, um die Details für einen bestimmten Wiederherstellungspunkt anzuzeigen.

So zeigen Sie einen bestimmten Wiederherstellungspunkt an

1. Navigieren Sie in der AppAssure Core Console zu der geschützten Maschine, für die Sie Wiederherstellungspunkte anzeigen möchten.
2. Klicken Sie auf die Registerkarte „Wiederherstellungspunkte“.
3. Klicken Sie auf das Symbol mit der rechten spitzen Klammer > neben einem Wiederherstellungspunkt in der Liste, um die Ansicht zu erweitern.

   Sie können ausführlichere Informationen zum Inhalt von Wiederherstellungspunkten der ausgewählten Maschine anzeigen sowie auf mehrere Vorgänge zugreifen, die für einen Wiederherstellungspunkt durchgeführt werden können (siehe Beschreibung in der folgenden Tabelle).

Tabelle 64.

Info	Beschreibung
Aktionen	Das Menü „Aktionen“ enthält die folgenden Vorgänge, die Sie für den ausgewählten Wiederherstellungspunkt durchführen können: **Bereitstellen**. Wählen Sie diese Option aus, um den ausgewählten Wiederherstellungspunkt bereitzustellen. Weitere Informationen finden Sie unter Bereitstellen eines Wiederherstellungspunktes für eine Windows-Maschine. **Export**. Mit der Option „Export“ können Sie den ausgewählten Wiederherstellungspunkt nach ESXi, VMware Workstation, HyperV oder VirtualBox exportieren. Weitere Informationen finden Sie unter Exportieren von Daten aus einer Windows-Maschine in eine virtuelle Maschine. **Wiederherstellen**. Wählen Sie diese Option aus, um eine Wiederherstellung aus dem ausgewählten Wiederherstellungspunkt auf ein bestimmtes Volume durchzuführen. Weitere Informationen finden Sie unter Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung. **Überprüfen.** Wählen Sie diese Option aus, wenn auf der geschützten Maschine SQL Server installiert ist, um eine Prüfsummenprüfung oder eine Bereitstellbarkeitsprüfung zu erzwingen. Weitere Informationen finden Sie unter Erzwingen von Prüfsummenprüfungen für Exchange Server-Wiederherstellungspunkte. Wählen Sie diese Option aus, wenn auf der geschützten Maschine Exchange Server installiert ist, um eine Anfügbarkeitsprüfung zu erzwingen. Weitere Informationen finden Sie unter Erzwingen einer Bereitstellbarkeitsprüfung für eine Exchange-Datenbank.
Inhalt	Der Bereich „Inhalt“ umfasst eine Zeile für jedes Volume im erweiterten Wiederherstellungspunkt, in der die folgenden Informationen für jedes Volume aufgelistet werden: **Status**. Zeigt den aktuellen Status des Wiederherstellungspunkts an. **Titel**. Zeigt eine Liste der Volumes im Wiederherstellungspunkt an. **Typ**. Zeigt an, ob der angegebene Wiederherstellungspunkt ein Basisimage oder ein inkrementeller (differenzieller) Snapshot ist. **Größe**. Zeigt den Speicherplatz an, den der Wiederherstellungspunkt im Repository belegt.

4 Klicken Sie auf das Symbol mit der rechten spitzen Klammer > neben einem Volume im ausgewählten Wiederherstellungspunkt, um die Ansicht zu erweitern.

Sie können die in der folgenden Tabelle beschriebenen Informationen für das ausgewählte Volume im erweiterten Wiederherstellungspunkt anzeigen.

Tabelle 65.

Textfeld	Beschreibung
Titel	Gibt das jeweilige Volume im Wiederherstellungspunkt an.
Dateisystem	Gibt den Dateisystemtyp für das ausgewählte Volume an.
Rohkapazität	Gibt die Größe des unformatierten Speicherplatzes im gesamten Volume an.
Formatierte Kapazität	Gibt die Größe des Speicherplatzes im Volume an, der nach der Formatierung des Volumes für Daten verfügbar ist.
Verwendete Kapazität	Gibt die Größe des Speicherplatzes an, der derzeit im Volume verwendet wird.

Bereitstellen eines Wiederherstellungspunktes für eine Windows-Maschine

In AppAssure können Sie einen Wiederherstellungspunkt für eine Windows-Maschine bereitstellen, um über ein lokales Dateisystem auf gespeicherte Daten zuzugreifen.

HINWEIS: Beim Bereitstellen von Wiederherstellungspunkten von Daten, die aus Windows-Maschinen wiederhergestellt wurden, für die die Deduplizierung von Daten aktiviert ist, müssen Sie darauf achten, dass die Deduplizierung auch im Core-Server aktiviert ist.

So stellen Sie einen Wiederherstellungspunkt für eine Windows-Maschine bereit

1 Navigieren Sie in der AppAssure Core Console zu der Maschine, die in einem lokalen Dateisystem bereitgestellt werden soll.

Die Registerkarte „Zusammenfassung“ für die ausgewählte Maschine wird angezeigt.

2 Klicken Sie auf die Registerkarte „Wiederherstellungspunkte“.

3 Klicken Sie in der Liste der Wiederherstellungspunkte auf die rechte spitze Klammer >, um den Wiederherstellungspunkt zu erweitern, der bereitgestellt werden soll.

4 Klicken Sie in den erweiterten Details für diesen Wiederherstellungspunkt auf **Bereitstellen**.

Das Dialogfeld „Wiederherstellungspunkte bereitstellen“ wird angezeigt.

5 Bearbeiten Sie im Dialogfeld „Wiederherstellungspunkt bereitstellen“ die Optionen für die Bereitstellung eines Wiederherstellungspunkts (siehe folgende Tabelle).

Tabelle 66.

Option	Beschreibung
Speicherort für Bereitstellung Lokaler Ordner	Geben Sie den Pfad an, der für den Zugriff auf den bereitgestellten Wiederherstellungspunkt verwendet wird.
Bereitstellungsoptionen: Bereitstellungstyp	Geben Sie an, wie der Datenzugriff für den bereitgestellten Wiederherstellungspunkt erfolgen soll: • Schreibgeschützt bereitstellen • Schreibgeschützt bereitstellen mit vorherigen Schreibvorgängen • Mit Schreibzugriff bereitstellen
Volume-Images	Geben Sie die Volume-Images an, die bereitgestellt werden sollen.
Windows-Freigabe für diese Bereitstellung erstellen	(Optional) Aktivieren Sie das Kontrollkästchen, um festzulegen, ob der bereitgestellte Wiederherstellungspunkt freigegeben wird, und legen Sie dann die entsprechenden Zugriffsrechte fest, einschließlich Freigabename und zugelassene Gruppen.

6 Klicken Sie auf **Bereitstellen**, um den Wiederherstellungspunkt bereitzustellen.

HINWEIS: Wenn Sie Verzeichnisse oder Dateien eines bereitgestellten Wiederherstellungspunkts auf eine andere Windows-Maschine kopieren möchten, können Sie sie in Windows-Explorer mit den Standardberechtigungen oder den ursprünglichen Dateizugriffsberechtigungen kopieren. Entsprechende Details finden Sie in den Abschnitten Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer bis Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer und Beibehalten der Berechtigungen.

7 Während die Aufgabe verarbeitet wird, können Sie den Fortschritt im Dropdown-Menü „Aktive Aufgaben“ der Core Console sowie ausführliche Information auf der Registerkarte „Ereignisse“ anzeigen. Weitere Informationen zur Überwachung von AppAssure-Ereignissen finden Sie unter Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen.

Aufheben der Bereitstellung ausgewählter Wiederherstellungspunkte

Führen Sie die folgenden Schritte aus, um die Bereitstellung ausgewählter Wiederherstellungspunkte aufzuheben, die im Core bereitgestellt wurden.

HINWEIS: Das Aufheben der Bereitstellung eines remote bereitgestellten Wiederherstellungspunkts wird auch *Trennen* genannt.

So heben Sie die Bereitstellung bestimmter Wiederherstellungspunkte auf

1. Klicken Sie in der AppAssure Core Console im Dropdown-Menü „Extras“ auf **Bereitstellungen**.

   Die Seite „Bereitstellungen“ wird angezeigt. Sie enthält einen Bereich für lokale Bereitstellungen (im Core bereitgestellte Wiederherstellungspunkte) und einen Bereich für Remote-Bereitstellungen (mit dem Local Mount Utility bereitgestellte Wiederherstellungspunkte). In der Liste des jeweiligen Bereichs werden die jeweils bereitgestellten Wiederherstellungspunkte angezeigt.

2. Führen Sie für die Wiederherstellungspunkte, deren Bereitstellung aufgehoben werden soll, die folgenden Schritte aus:

   - Klicken Sie auf im Bereich **Lokale Bereitstellungen** neben den einzelnen lokal bereitgestellten Wiederherstellungspunkten in der Liste, deren Bereitstellung aufgehoben werden soll, auf **Bereitstellung aufheben**.
   - Klicken Sie auf im Bereich **Remote-Bereitstellungen** neben den einzelnen remote bereitgestellten Wiederherstellungspunkten in der Liste, deren Bereitstellung aufgehoben werden soll, auf **trennen**.

3. Klicken Sie im Dialogfeld „Aufheben der Bereitstellung des Wiederherstellungspunktes“ zur Bestätigung auf **Ja**.

4. Vergewissern Sie sich, dass die zuvor bereitgestellten Wiederherstellungspunkte nicht mehr in der Liste „Lokale Bereitstellungen“ bzw. „Remote-Bereitstellungen“ angezeigt werden.

Aufheben der Bereitstellung aller Wiederherstellungspunkte

Führen Sie die folgenden Schritte aus, um die Bereitstellung aller Wiederherstellungspunkte aufzuheben, die im Core bereitgestellt wurden.

HINWEIS: Das Aufheben der Bereitstellung eines remote bereitgestellten Wiederherstellungspunkts wird auch *Trennen* genannt.

So heben Sie die Bereitstellung aller Wiederherstellungspunkte auf

1. Klicken Sie in der AppAssure Core Console im Dropdown-Menü „Extras“ auf **Bereitstellungen**.

   Die Seite „Bereitstellungen“ wird angezeigt. Sie enthält einen Bereich für lokale Bereitstellungen (im Core bereitgestellte Wiederherstellungspunkte) und einen Bereich für Remote-Bereitstellungen (mit dem Local Mount Utility bereitgestellte Wiederherstellungspunkte). In der Liste des jeweiligen Bereichs werden die jeweils bereitgestellten Wiederherstellungspunkte angezeigt.

2. Führen Sie für die Wiederherstellungspunkte, deren Bereitstellung aufgehoben werden soll, die folgenden Schritte aus:

   - Klicken Sie im Bereich „Lokale Bereitstellungen“ auf **Alle Bereitstellungen aufheben**, um die Bereitstellung aller lokal bereitgestellten Wiederherstellungspunkte aufzuheben.
   - Klicken Sie im Bereich „Remote-Bereitstellungen“ auf **Alle trennen**, um die Bereitstellung aller remote bereitgestellten Wiederherstellungspunkte aufzuheben.

3 Klicken Sie im Dialogfeld „Aufheben der Bereitstellung aller Wiederherstellungspunkte“ zur Bestätigung auf **Ja**.

4 Überprüfen Sie, ob die Bereitstellung aller lokal oder remote bereitgestellten Wiederherstellungspunkte aufgehoben bzw. die Verbindung zu den Wiederherstellungspunkten getrennt wurde.

Bereitstellen eines Wiederherstellungspunkt-Volumes für eine Linux-Maschine

Mit dem AppAssure-Dienstprogramm `aamount` können Sie ein Volume eines Wiederherstellungspunkts auf einer Linux-Maschine als lokales Volume bereitstellen.

HINWEIS: Versuchen Sie dabei nicht, Wiederherstellungspunkte im Ordner „/tmp“ bereitzustellen, da dieser die aavdisk-Dateien enthält.

So stellen Sie ein Wiederherstellungspunkt-Volumes für eine Linux-Maschine bereit

1 Erstellen Sie ein neues Verzeichnis für die Bereitstellung des Wiederherstellungspunkts (z. B. mit dem Befehl `mkdir`).

2 Vergewissern Sie sich, dass das Verzeichnis vorhanden ist (z. B. mit dem Befehl `ls`).

3 Führen Sie das AppAssure-Dienstprogramm `aamount` als Root oder als Superuser aus, z. B.:

```
sudo aamount
```

4 Geben Sie an der AppAssure-Eingabeaufforderung den folgenden Befehl ein, um die geschützten Maschinen aufzulisten.

```
lm
```

5 Geben Sie die IP-Adresse oder den Hostnamen des AppAssure Core-Servers ein.

6 Geben Sie die Anmeldeinformationen (Benutzername und Kennwort) für den Core-Server ein.

Daraufhin wird eine Liste der Maschinen angezeigt, die vom AppAssure-Server geschützt werden. Die Liste enthält für jede Maschine die folgenden Informationen: laufende Zeilennummer, Host/IP-Adresse und ID-Nummer für die Maschine.

Beispiel: 293cc667-44b4-48ab-91d8-44bc74252a4f

7 Geben Sie den folgenden Befehl ein, um die für eine bestimmte Maschine verfügbaren Wiederherstellungspunkte anzuzeigen:

```
lr <Zeilennummer_der_Maschine>
```

HINWEIS: Sie können in diesem Befehl auch die ID-Nummer der Maschine anstelle der laufenden Zeilennummer angeben.

Daraufhin werden die Basiswiederherstellungspunkte und die inkrementellen Wiederherstellungspunkte für die betreffende Maschine aufgelistet. Die Liste umfasst die laufende Zeilennummer, Datum/Zeitstempel, Speicherort des Volumes, Größe des Wiederherstellungspunkts und eine ID-Nummer für das Volume mit einer laufenden Nummer am Ende, die den Wiederherstellungspunkt kennzeichnet,

z. B. 293cc667-44b4-48ab-91d8-44bc74252a4f:2.

8 Geben Sie den folgenden Befehl ein, um den angegebenen Wiederherstellungspunkt auszuwählen und im angegebenen Bereitstellungspunkt/-pfad bereitzustellen.

```
m <ID-Nummer_für_Volume-Wiederherstellungspunkt> <Pfad>
```

> **HINWEIS:** Sie können im Befehl auch die Zeilennummer anstelle der ID-Nummer für den Wiederherstellungspunkt angeben, um den Wiederherstellungspunkt anzugeben. In diesem Fall müssen Sie die Zeilennummer für Agent/Maschine (in der lm-Ausgabe), gefolgt von der Zeilennummer des Wiederherstellungspunkts und dem Volume-Buchstaben und dahinter den Pfad angeben, z. B. „m <Zeilennummer_für_Maschine> <Zeilennummer_für_Wiederherstellungspunkt> <Volume-Buchstabe> <Pfad>“. Wenn die `lm`-Ausgabe beispielsweise drei Agent-Maschinen auflistet, Sie den Befehl `lr` für Nummer 2 eingeben und Sie den Wiederherstellungspunkt 23 mit Volume B in /tmp/mount_dir bereitstellen, lautet der Befehl:
> `m 2 23 b /tmp/mount_dir`

9 Um festzustellen, ob die Bereitstellung erfolgreich durchgeführt wurde, geben Sie den folgenden Befehl ein, der das angehängte Remote-Volume auflisten sollte:

```
l
```

Aufheben der Bereitstellung eines Wiederherstellungspunkts auf einer Linux-Maschine

Führen Sie die folgenden Schritte aus, um die Bereitstellung eines Wiederherstellungspunkt auf einer Linux-Maschine aufzuheben.

So heben Sie die Bereitstellung eines Wiederherstellungspunkts für eine Linux-Maschine auf

1 Führen Sie das AppAssure-Dienstprogramm `aamount` als Root oder als Superuser aus, z. B.:

```
sudo aamount
```

2 Geben Sie an der AppAssure-Eingabeaufforderung den folgenden Befehl ein, um die geschützten Maschinen aufzulisten.

```
lm
```

3 Geben Sie die IP-Adresse oder den Hostnamen des AppAssure Core-Servers ein.

4 Geben Sie die Anmeldeinformationen (Benutzername und Kennwort) für den Core-Server ein.

Daraufhin wird eine Liste der Maschinen angezeigt, die vom AppAssure-Server geschützt werden.

5 Geben Sie den folgenden Befehl ein, um die für eine bestimmte Maschine verfügbaren Wiederherstellungspunkte anzuzeigen:

```
lr <Zeilennummer_der_Maschine>
```

> **HINWEIS:** Sie können in diesem Befehl auch die ID-Nummer der Maschine anstelle der laufenden Zeilennummer angeben.

Daraufhin werden die Basiswiederherstellungspunkte und die inkrementellen Wiederherstellungspunkte für die betreffende Maschine aufgelistet. Die Liste umfasst die laufende Zeilennummer, Datum/Zeitstempel, Speicherort des Volumes, Größe des Wiederherstellungspunkts und eine ID-Nummer für das Volume mit einer laufenden Nummer am Ende, die den Wiederherstellungspunkt kennzeichnet,

z. B. 293cc667-44b4-48ab-91d8-44bc74252a4f:2.

6 Führen Sie den Befehl `l oder list` aus, um eine Liste der bereitgestellten NBD-Geräte (Network Block Device) abzurufen. Wenn Sie einen Wiederherstellungspunkt bereitstellen, wird nach der Ausführung des Befehls `l oder list` ein Pfad zum NBD-Gerät ausgegeben.

7 Geben Sie den folgenden Befehl ein, um die Bereitstellung eines Wiederherstellungspunkts aufzuheben.

```
unmount <Pfad_des_NBD-Geräts>
```

8 Führen Sie den Befehl `l oder list` aus, um zu überprüfen, ob die Bereitstellung des Wiederherstellungspunkts erfolgreich aufgehoben wurde.

Entfernen von Wiederherstellungspunkten

Sie können Wiederherstellungspunkte für eine bestimmte Maschine einfach aus dem Repository entfernen. Beim Löschen von Wiederherstellungspunkten in AppAssure können Sie eine der folgenden Optionen angeben.

- **Alle Wiederherstellungspunkte löschen.** Entfernt alle Wiederherstellungspunkte für die ausgewählte Agent-Maschine aus dem Repository.
- **Bereich von Wiederherstellungspunkten löschen**. Entfernt alle Wiederherstellungspunkte in einem angegebenen Bereich vor dem aktuellen, bis einschließlich zum Basisimage, d. h. alle Daten auf der Maschine sowie alle Wiederherstellungspunkte nach dem aktuellen bis hin zum nächsten Basisimage.

ⓘ **HINWEIS:** Gelöschte Wiederherstellungspunkte können nicht wiederhergestellt werden.

So entfernen Sie Wiederherstellungspunkte

1. Navigieren Sie in der AppAssure Core Console zu der Maschine, für die Sie Wiederherstellungspunkte anzeigen möchten.
2. Klicken Sie auf die Registerkarte „Wiederherstellungspunkte“.
3. Klicken Sie auf das Menü **Aktionen**.
4. Wählen Sie eine der folgenden Optionen:
   - Um alle derzeit gespeicherten Wiederherstellungspunkte zu löschen, klicken Sie auf **Alle löschen**.
   - Um die Wiederherstellungspunkte in einem bestimmten Datenbereich zu löschen, klicken Sie auf **Bereich löschen**.

     Das Dialogfeld „Löschen“ wird angezeigt.

     - Geben Sie im Dialogfeld „Bereich löschen“ den Bereich der Wiederherstellungspunkte an, den Sie löschen möchten. Geben Sie dazu ein Startdatum und eine Startzeit sowie ein Enddatum und eine Endzeit an. Klicken Sie anschließend auf **Löschen**.

Löschen einer verwaisten Wiederherstellungspunktkette

Bei einem verwaisten Wiederherstellungspunkt handelt es sich um einen inkrementellen Snapshot, der keinem Basisimage zugeordnet ist. Nachfolgende Snapshots bauen jedoch weiterhin auf diesem Wiederherstellungspunkt auf. Ohne das Basisimage sind die entstehenden Wiederherstellungspunkte jedoch unvollständig und enthalten höchstwahrscheinlich nicht die erforderlichen Daten für eine Wiederherstellung. Diese Wiederherstellungspunkte werden als Teil der verwaisten Wiederherstellungspunktkette angesehen. In dieser Situation sollte idealerweise die Kette gelöscht und ein neues Basisimage erstellt werden.

Weitere Informationen zum Erzwingen eines Basisimage finden Sie unter Erzwingen eines Snapshots.

So löschen Sie eine verwaiste Wiederherstellungspunktkette

1. Navigieren Sie in der AppAssure Core Console zu der geschützten Maschine, für die Sie die verwaiste Wiederherstellungspunktkette löschen möchten.
2. Klicken Sie auf die Registerkarte „Wiederherstellungspunkte“.
3. Erweitern Sie unter „Wiederherstellungspunkte“ den verwaisten Wiederherstellungspunkt.

   Ein solcher Wiederherstellungspunkt weist in der Spalte „Typ“ den Eintrag „Inkrementell, Verwaist“ auf.
4. Klicken Sie neben „Aktionen“ auf **Löschen**.

   Das Fenster „Wiederherstellungspunkte löschen“ wird angezeigt.
5. Klicken Sie im Dialogfeld „Wiederherstellungspunkte löschen“ auf **Ja**.

△ **VORSICHT: Durch Löschen dieses Wiederherstellungspunkts wird die gesamte Wiederherstellungspunktkette mit allen inkrementellen Wiederherstellungspunkten davor oder danach bis zum nächsten Basisimage gelöscht. Dieser Vorgang kann nicht rückgängig gemacht werden.**

Die verwaiste Wiederherstellungspunktkette wird gelöscht.

Erzwingen eines Snapshots

Durch das Erzwingen eines Snapshots können Sie eine Datenübertragung für die aktuelle geschützte Maschine erzwingen. Wenn Sie eine Snapshot-Erstellung erzwingen, wird die Übertragung entweder sofort gestartet oder zur Warteschlange hinzugefügt. Dabei werden nur die Daten übertragen, die seit einem vorherigen Wiederherstellungspunkt geändert wurden. Wenn kein früherer Wiederherstellungspunkt verfügbar ist, werden alle Daten auf den geschützten Volumes übertragen. Dies wird auch als Basisimage bezeichnet.

HINWEIS: AppAssure unterstützt Windows 8, Windows 8.1, Windows Server 2012 und Windows Server 2012 R2 für Basis- und inkrementelle Übertragungen.

So erzwingen Sie einen Snapshot

1. Navigieren Sie in der AppAssure Core Console zu der Maschine oder dem Cluster, für die/den Sie einen Snapshot erzwingen möchten.
2. Geben Sie auf der Registerkarte „Zusammenfassung“ im Abschnitt „Volumes“ die Volumes an, für die ein Snapshot erstellt werden soll, und klicken Sie dann auf die Schaltfläche **Snapshot erzwingen** oder die Schaltfläche **Basisimage erzwingen**.

Tabelle 67.

Option	Beschreibung
Snapshot erzwingen	Erstellt einen inkrementellen Snapshot der Daten, die seit der Erstellung des letzten Snapshots aktualisiert wurden.
Basisimage erzwingen	Erstellt einen vollständigen Snapshot aller Daten auf den Volumes der Maschine.

Verwalten von SQL- und Exchange-Servern

Wenn SQL Server und Exchange Server geschützt werden, gibt es spezielle Funktionen für diese Servertypen, die Sie durchführen können. Dazu gehören:

- **Kürzung des Serverprotokolls erzwingen.** SQL Server sowie Exchange Server enthalten Serverprotokolle. Beim Kürzen von SQL-Protokollen wird der verfügbare Speicherplatz auf dem Server ermittelt. Beim Kürzen von Exchange-Serverprotokollen wird der verfügbare Speicherplatz ermittelt und mehr Speicherplatz auf dem Server freigegeben. Informationen zum Erzwingen der Protokollkürzung finden Sie unter Erzwingen einer Protokollkürzung für eine SQL- oder Exchange-Maschine.
- **Anmeldeinformationen für den jeweiligen Server festlegen.** Bei Exchange-Servern können Sie die Anmeldeinformationen für die geschützte Maschine auf der Registerkarte „Zusammenfassung“ für den geschützten Server festlegen. Bei SQL-Servern können Sie Anmeldeinformationen für eine einzelne geschützte SQL-Servermaschine oder Standardanmeldeinformationen für alle geschützten SQL-Server festlegen.
    - Informationen zum Festlegen der Anmeldeinformationen für Exchange-Server finden Sie unter Festlegen der Anmeldeinformationen für Exchange-Server.
    - Informationen zum Festlegen der Anmeldeinformationen für SQL-Server finden Sie unter Festlegen der Anmeldeinformationen für SQL-Server.
    - Informationen zum Durchführen anderer Aktionen, die für alle geschützte Agenten auf der Registerkarte „Zusammenfassung“ zugänglich sind, finden Sie unter Informationen zur Registerkarte „Zusammenfassung“.

Festlegen der Anmeldeinformationen für Exchange-Server

Wenn die Daten eines Microsoft Exchange-Servers geschützt werden, können Sie die Anmeldeinformationen in der AppAssure Core Console konfigurieren.

So legen Sie die Anmeldeinformationen für einen Exchange-Server fest

1. Nachdem Sie die Exchange Server-Maschine unter Schutz gestellt haben, gehen Sie zur AppAssure Core Console und wählen Sie die Maschine im Navigationsbereich aus.

   Die Registerkarte „Zusammenfassung“ für die Maschine wird angezeigt.

2. Klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü **Aktionen** auf **Exchange** und wählen Sie im kontextsensitiven Dropdown-Menü die gewünschte Aktion aus.

3. Klicken Sie auf **Anmeldeinformationen einrichten**, um die Anmeldeinformationen für einen einzelnen Exchange-Server festzulegen, und führen Sie im Dialogfeld „Exchange-Anmeldeinformationen bearbeiten“ die folgenden Schritte aus:

   a. Geben Sie im Textfeld „Benutzername“ den Benutzernamen eines Benutzers mit Berechtigungen für den Exchange-Server ein, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).

   b. Geben Sie im Textfeld „Kennwort“ das Kennwort für den Benutzernamen ein, der für die Verbindung zum Exchange-Server angegeben wurde.

   c. Klicken Sie auf **OK** um die Einstellungen zu bestätigen und das Dialogfeld zu schließen.

Festlegen der Anmeldeinformationen für SQL-Server

Wenn die Daten eines SQL-Servers geschützt werden, können Sie die Anmeldeinformationen in der AppAssure Core Console konfigurieren.

So legen Sie die Anmeldeinformationen für SQL-Server fest

1. Nachdem Sie die SQL Server-Maschine unter Schutz gestellt haben, gehen Sie zur AppAssure Core Console und wählen Sie die Maschine im Navigationsbereich aus.

   Die Registerkarte „Zusammenfassung“ für die Maschine wird angezeigt.

2. Klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü **Aktionen** auf „SQL“ und wählen Sie im kontextsensitiven Dropdown-Menü die gewünschte Aktion aus.

   - Klicken Sie auf **Standardanmeldeinformationen für alle Instanzen festlegen**, wenn Sie die Standardanmeldeinformationen für alle SQL Server-Datenbankinstanzen festlegen möchten, und führen Sie im Dialogfeld „Standardanmeldeinformationen bearbeiten“ die folgenden Schritte aus:

     a. Geben Sie im Textfeld „Benutzername“ den Benutzernamen eines Benutzers mit Berechtigungen für alle SQL-Server ein, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).

     b. Geben Sie im Textfeld „Kennwort“ das Kennwort für den Benutzernamen ein, der für die Verbindung zum SQL-Server angegeben wurde.

     c. Klicken Sie auf **OK** um die Einstellungen zu bestätigen und das Dialogfeld zu schließen.

   - Klicken Sie auf **Anmeldeinformationen für Instanz festlegen**, wenn Sie die Anmeldeinformationen für eine einzelne SQL Server-Datenbankinstanz festlegen möchten, und führen Sie im Dialogfeld „Anmeldeinformationen für Instanz bearbeiten“ die folgenden Schritte aus:

     a. Wählen Sie den Typ der Anmeldeinformationen aus („Standard“, „Windows“ oder „SQL“).

b Geben Sie im Textfeld „Benutzername“ den Benutzernamen eines Benutzers mit Berechtigungen für den SQL-Server ein, z. B. „Administrator“ (bzw. [Domänenname]\Administrator, wenn sich die Maschine in einer Domäne befindet).

c Geben Sie im Textfeld „Kennwort“ das Kennwort für den Benutzernamen ein, der für die Verbindung zum SQL-Server angegeben wurde.

d Klicken Sie auf **OK** um die Einstellungen zu bestätigen und das Dialogfeld zu schließen.

Informationen zum Wiederherstellen von Daten aus Wiederherstellungspunkten

AppAssure schützt Daten auf Windows- und Linux-Maschinen. Die Sicherungen geschützter Agent-Maschinen werden im AppAssure Core als Wiederherstellungspunkte gespeichert. Mithilfe dieser Wiederherstellungspunkte können Sie Daten wiederherstellen. Dafür gibt es drei Möglichkeiten.

In der AppAssure Core Console können Sie ganze Volumes eines Wiederherstellungspunkts für ein Nicht-System-Volume wiederherstellen, wobei die Volumes auf der Zielmaschine ersetzt werden. Dies ist für Windows- und Linux-Maschinen möglich. Weitere Informationen finden Sie unter Wiederherstellen von Volumes aus einem Wiederherstellungspunkt.

Sie können über die Befehlszeile auf dem Linux-Agenten auch ganze Volumes von Linux-Maschinen aus Wiederherstellungspunkten wiederherstellen. Weitere Informationen zur Verwendung des Befehlszeilenprogramms „aamount“ finden Sie unter Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile.

Sie können ein Volume, das das Betriebssystem enthält, nicht direkt aus einem Wiederherstellungspunkt wiederherstellen, da die Maschine, auf der die Wiederherstellung erfolgt, bei der Wiederherstellung das Betriebssystem und die Treiber benötigt. Wenn Sie ein System-Volume (z. B. das Laufwerk C: der Agent-Maschine) aus einem Wiederherstellungspunkt wiederherstellen möchten, müssen Sie eine BMR-Wiederherstellung (Bare Metal Restore) durchführen. Dabei wird ein startfähiges Image aus dem Wiederherstellungspunkt erstellt, das Betriebssystem und Konfigurationsdateien sowie Daten enthält. Anschließend wird die Zielmaschine mit dem startfähigen Image gestartet, um die eigentliche Wiederherstellung durchzuführen. Das Startimage hängt vom Betriebssystem der Maschine ab, die wiederhergestellt werden soll (Windows oder Linux).

Informationen zum Wiederherstellen eines Wiederherstellungspunkts für ein System-Volume auf einer Windows-Maschine finden Sie unter Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen.

Informationen zum Wiederherstellen eines Wiederherstellungspunkts für ein System-Volume auf einer Linux-Maschine finden Sie unter Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen.

Anstatt ganze Volumes wiederherzustellen, können Sie einen Wiederherstellungspunkt für eine Windows-Maschine bereitstellen sowie einzelne Ordner und Dateien durchsuchen, um nur bestimmte Dateien wiederherzustellen. Weitere Informationen finden Sie unter Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer. Informationen zum Beibehalten der ursprünglichen Dateiberechtigungen beim Wiederherstellen einzelner Dateien (z. B. beim Wiederherstellen eines Benutzerordners auf einem Dateiserver) finden Sie unter Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer und Beibehalten der Berechtigungen.

In diesem Abschnitt wird die Wiederherstellung von Daten auf physischen Maschinen behandelt. Weitere Information zum Exportieren geschützter Daten von Windows-Maschinen in virtuelle Maschinen finden Sie unter Information zum Exportieren geschützter Daten von Windows-Maschinen in virtuelle Maschinen.

HINWEIS: Bei der Wiederherstellung von Daten auf Windows-Maschinen müssen Sie darauf achten, dass die Deduplizierung auch im Core-Server aktiviert ist, wenn für das wiederhergestellte Volume die Windows-Datendeduplizierung aktiviert ist.

AppAssure unterstützt Windows 8, Windows 8.1, Windows Server 2012 und Windows Server 2012 R2 für normale Übertragungen (Basisimage und inkrementell) sowie für Datenwiederherstellung, BMR-Wiederherstellung und virtuelle Exporte.

Weitere Informationen zu den verschiedenartigen Volumes, die für Sicherung und Wiederherstellung unterstützt werden bzw. nicht unterstützt werden, finden Sie unter Einschränkungen bei der Unterstützung dynamischer Volumes und Basis-Volumes.

Wiederherstellen von Volumes aus einem Wiederherstellungspunkt

Sie können die Volumes einer geschützten Maschine aus den Wiederherstellungspunkten wiederherstellen, die im AppAssure Core gespeichert sind. In AppAssure 5.4 und höher wird dafür der Assistent zum Wiederherstellen einer Maschine verwendet.

HINWEIS: In früheren Releases wurde dieser Prozess als Rollback bezeichnet.

AppAssure unterstützt Schutz und Wiederherstellung von Maschinen mit EISA-Partitionen. Die Unterstützung wurde auch auf Maschinen mit Windows 8 und Windows 8.1 sowie Windows 2012 und Windows 2012 R2 erweitert, die Windows RE (Windows Recovery Environment) verwenden.

Sie können eine Wiederherstellung an jeder Stelle in der AppAssure Core Console starten, indem Sie auf das Symbol **Wiederherstellen** in der AppAssure-Schaltflächenleiste klicken. Wenn Sie so eine Wiederherstellung starten, müssen Sie die geschützte Maschine im Core angeben, die wiederhergestellt werden soll, und dann das Volume auswählen, das wiederhergestellt werden soll.

Sie können in der Benutzeroberfläche der Core Console auch eine bestimmte Maschine auswählen, die Wiederherstellungspunkte für Volumes der betreffenden Maschine erweitern und im gewünschten Wiederherstellungspunkt **Wiederherstellen** auswählen. Führen Sie die nachstehend beschriebenen Schritte ab Schritt 5 durch, wenn Sie so eine Wiederherstellung starten.

Wenn Sie einen Wiederherstellungspunkt auf einer Linux-Maschine wiederherstellen möchten, müssen Sie erst die Festplatte unmounten, auf der die Daten wiederhergestellt werden sollen.

Wenn Sie ein System-Volume aus einem Wiederherstellungspunkt oder Daten mithilfe einer Start-CD aus einem Wiederherstellungspunkt wiederherstellen möchten, müssen Sie eine BMR-Wiederherstellung (Bare Metal Restore) durchführen. Informationen zur BMR-Wiederherstellung finden Sie unter Grundlegende Informationen zur BMR-Wiederherstellung. Informationen zu den jeweils erforderlichen Komponenten für Windows- oder Linux-Betriebssysteme finden Sie unter Voraussetzungen für eine BMR-Wiederherstellung für Windows-Maschinen bzw. Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen. Sie können in der Core Console auf die BMR-Funktionen zugreifen (siehe Beschreibung in der Anleitung für das jeweilige Betriebssystem). Sie können auch mit dem Assistenten zum Wiederherstellen von Maschinen eine BMR-Wiederherstellung durchführen. Die folgende Vorgehensweise führt Sie zum entsprechenden Punkt im Assistenten, ab dem Sie die in Verwalten eines Windows-Start-Image und Starten einer BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine beschriebenen Schritte durchführen können.

Gehen Sie folgendermaßen vor, um Volumes aus einem Wiederherstellungspunkt wiederherzustellen.

So stellen Sie Volumes aus einem Wiederherstellungspunkt wieder her

1 Um ein Volume einer geschützten Maschine über das Symbol „Wiederherstellen“ wiederherzustellen, navigieren Sie zur Core Console und klicken Sie auf **Wiederherstellen** in der AppAssure-Schaltflächenleiste.

Der Assistent zum Wiederherstellen einer Maschine wird angezeigt.

2 Wählen Sie auf der Seite „Geschützte Maschinen“ die geschützte Maschine aus, für die Sie Daten wiederherstellen möchten, und klicken Sie dann auf **Weiter**.

> **HINWEIS:** Auf der geschützten Maschine muss die Agent-Software installiert sein. Außerdem müssen Wiederherstellungspunkte vorhanden sein, aus denen Daten wiederhergestellt werden können.

Die Seite „Wiederherstellungspunkte“ wird angezeigt.

3 Wählen Sie in der Liste der Wiederherstellungspunkte den Snapshot aus, der auf die Agent-Maschine wiederhergestellt werden soll.

- Über die Navigationsschaltflächen am Ende der Seite können Sie ggf. weitere Wiederherstellungspunkte anzeigen.
- Um die Anzahl der Wiederherstellungspunkte zu begrenzen, die auf der Seite „Wiederherstellungspunkte“ des Assistenten angezeigt werden, können Sie nach Volumes (falls definiert) oder nach Erstellungsdatum des Wiederherstellungspunkts filtern.

4 Klicken Sie auf einen Wiederherstellungspunkt, um ihn auszuwählen, und klicken Sie dann auf **Weiter**.

Die Seite „Ziel“ wird angezeigt.

5 Wählen Sie auf der Seite „Ziel“ die Maschine aus, auf die die Daten wiederhergestellt werden sollen. Gehen Sie dazu folgendermaßen vor:

- Wählen Sie **Wiederherstellung auf eine geschützte Maschine (nur Nicht-System-Volumes)** aus, wenn Sie Daten aus dem ausgewählten Wiederherstellungspunkt auf dieselbe Agent-Maschine (z. B. Maschine1) wiederherstellen möchten und die Volumes, auf die die Daten wiederhergestellt werden sollen, keine System-Volumes sind. Vergewissern Sie sich, dass die Zielmaschine (Maschine1) ausgewählt ist, und klicken Sie dann auf **Weiter**.

  Die Seite „Volume-Zuordnung“ wird angezeigt. Fahren Sie mit Schritt 9 fort.

- Wählen Sie **Wiederherstellung auf eine geschützte Maschine (nur Nicht-System-Volumes)** aus, wenn Sie Daten aus dem ausgewählten Wiederherstellungspunkt auf eine andere geschützte Maschine wiederherstellen möchten (um beispielsweise den Inhalt von Maschine2 durch den von Maschine1 zu ersetzen). Wählen Sie die Zielmaschine (z. B. Maschine2) in der Liste aus, und klicken Sie dann auf **Weiter**.

  Die Seite „Volume-Zuordnung“ wird angezeigt. Fahren Sie mit Schritt 9 fort.

- Wenn Sie Daten aus dem ausgewählten Wiederherstellungspunkt auf derselben Maschine oder mit einer Start-CD auf einer anderen Maschine wiederherstellen möchten, müssen Sie eine BMR-Wiederherstellung (Bare Metal Restore) durchführen. Informationen zur BMR-Wiederherstellung finden Sie unter Grundlegende Informationen zur BMR-Wiederherstellung.

  > **HINWEIS:** Um eine BMR-Wiederherstellung durchführen zu können, müssen abhängig vom Betriebssystem der Agent-Maschine, die wiederhergestellt werden soll, bestimmte Voraussetzungen erfüllt sein. Grundlegende Informationen zu diesen Voraussetzungen finden Sie unter Voraussetzungen für eine BMR-Wiederherstellung für Windows-Maschinen bzw. Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen.

  Wählen Sie **Wiederherstellung auf einer beliebigen Zielmaschine mit einer Start-CD** aus, wenn die Volumes, die wiederhergestellt werden sollen, nicht das System-Volume umfassen. Bei Auswahl dieser Option werden Sie aufgefordert, eine Start-CD zu erstellen.

  - Klicken Sie auf **Weiter**, um fortzufahren und mit dem Assistenten zum Wiederherstellen einer Maschine eine Start-CD mit den Daten des ausgewählten Wiederherstellungspunkts zu erstellen, und gehen Sie zu Verwalten eines Windows-Start-Image und Starten einer BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine.
  - Wenn die Start-CD bereits erstellt und die Zielmaschine bereits mit der Start-CD gestartet wurde, gehen Sie zu Schritt 8 im Abschnitt Verwalten eines Windows-Start-Image und Starten einer BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine.

- Wenn Sie ein System-Volume (z. B. das Laufwerk C: der Agent-Maschine namens Maschine1) aus einem Wiederherstellungspunkt wiederherstellen möchten, handelt es sich ebenfalls um eine

BMR-Wiederherstellung (Bare Metal Restore). Wählen Sie **Wiederherstellung auf einer beliebigen Zielmaschine mit einer Start-CD** aus. Bei Auswahl dieser Option werden Sie aufgefordert, eine Start-CD zu erstellen.

- Klicken Sie auf Weiter, um fortzufahren und mit dem Assistenten zum Wiederherstellen einer Maschine eine Start-CD mit den Daten des ausgewählten Wiederherstellungspunkts zu erstellen, und fahren Sie mit Verwalten eines Windows-Start-Image und Starten einer BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine fort.
- Gehen Sie zu Schritt 6, wenn Sie die Start-CVD bereits erstellt haben.

6 Starten Sie die Maschine, die Sie wiederherstellen möchten, mit der Start-CD. Weitere Informationen zur BMR-Wiederherstellung auf einer Windows-Maschine finden Sie unter Laden der Start-CD und Starten der Zielmaschine. Weitere Informationen zur BMR-Wiederherstellung auf einer Linux-Maschine finden Sie unter Laden der Live DVD und Starten der Zielmaschine.

7 Wählen Sie auf dem Core-Server auf der Seite „Ziel“ des Assistenten zum Wiederherstellen einer Maschine **Ich habe bereits eine Start-CD für die Zielmaschine** aus und geben Sie die Informationen zu der Maschine ein, zu der eine Verbindung hergestellt werden soll (siehe Beschreibung in der folgenden Tabelle).

Tabelle 68.

Textfeld	Beschreibung
IP-Adresse	Die IP-Adresse der Maschine, die wiederhergestellt werden soll. Diese Adresse ist mit der IP-Adresse identisch, die im URC angezeigt wird.
Authentifizierungs-schlüssel	Das jeweilige Kennwort für die Verbindung zum ausgewählten Server. Dieses Kennwort ist mit dem Authentifizierungsschlüssel identisch, der im URC angezeigt wird.

8 Klicken Sie auf **Weiter**.

Wenn die eingegebenen Verbindungsinformationen mit den URC-Informationen übereinstimmen und Core und Zielserver sich gegenseitig einwandfrei im Netzwerk finden, werden die Volumes des ausgewählten Wiederherstellungspunkt geladen und die Seite „Datenträgerzuordnung“ geladen.

Fahren Sie mit Schritt 8 im Abschnitt Verwalten eines Windows-Start-Image und Starten einer BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine fort, um die BMR-Wiederherstellung mit dem Assistenten zum Wiederherstellen einer Maschine durchzuführen.

HINWEIS: Obwohl AppAssure FAT32- und ReFS-Partitionen unterstützt, werden zurzeit lediglich vollständige Wiederherstellung und BMR-Wiederherstellung unterstützt, da es bei ReFS Treibereinschränkungen gibt, sodass Wiederherstellung, VM-Export usw. im Benutzermodus implementiert sind. Wenn ein Core mindestens ein Agent-Volume mit dem ReFS-Dateisystem schützt, sollte der Core unter Windows 8/2012 installiert werden, da diese Versionen eine native Unterstützung von ReFS enthalten. Andernfalls ist die Funktionalität eingeschränkt, sodass Vorgänge (z. B. das Bereitstellen eines Volume-Image) nicht funktionieren. In diesem Fall werden in der AppAssure Core Console entsprechende Fehlermeldungen angezeigt.

Eine BMR-Wiederherstellung (Bare Metal Restore) der Festplattenkonfiguration für Speicherplätze (eine Funktion von Windows 8.1) wird in diesem Release ebenfalls nicht unterstützt. Details finden Sie im *Dell AppAssure Bereitstellungshandbuch*.

9 Wählen Sie auf der Seite „Volume-Zuordnung“ für jedes Volume im Wiederherstellungspunkt, das wiederhergestellt werden soll, das gewünschte Ziel-Volume aus. Wählen Sie in der Spalte „Ziel-Volumes“ **Nicht wiederherstellen** aus, wenn ein Volume nicht wiederhergestellt werden soll.

10 Wählen Sie **Erweiterte Optionen anzeigen** aus und führen Sie die folgenden Aktionen aus:

- Wählen Sie **Live Recovery** aus, um eine Wiederherstellung auf Windows-Maschinen mit Live Recovery durchzuführen.

  Mit der Live Recovery-Technologie für eine sofortige Wiederherstellung in AppAssure können Sie Daten aus gespeicherten Wiederherstellungspunkten von Windows-Maschinen (einschließlich

Microsoft Windows-Speicherplätzen) auf physische oder virtuelle Maschinen wiederherstellen. Live Recovery ist für Linux-Maschinen nicht verfügbar.

- Wählen Sie **Aufheben der Bereitstellung erzwingen** aus, um die Bereitstellung aufzuheben.

  Wenn Sie die Bereitstellung vor der Datenwiederherstellung nicht aufheben, kann die Wiederherstellung mit der Fehlermeldung fehlschlagen, dass ein Volume verwendet wird.

11 Fahren Sie mit Schritt 12 fort.

12 Wenn die wiederherzustellenden Volumes SQL- oder Microsoft Exchange-Datenbanken enthalten, werden Sie auf der Seite „Datenbankbereitstellungen aufheben“ aufgefordert, die Volumes zu unmounten. Wählen Sie ggf. **Alle Datenbanken nach der Wiederherstellung des Wiederherstellungspunkts wieder bereitstellen** aus, wenn die Datenbanken nach der Wiederherstellung wieder bereitgestellt werden sollen. Klicken Sie anschließend auf **Fertigstellen**.

13 Klicken Sie auf **OK**, um die Statusmeldung mit dem Hinweis zu bestätigen, dass die Wiederherstellung gestartet wurde.

14 Klicken Sie ggf. in der Core Console auf **Ereignisse**, um den Fortschritt der Wiederherstellung zu überwachen. Weitere Informationen finden Sie unter Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen.

Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile

In AppAssure, können Sie Volumes von geschützten Linux-Maschinen mit dem Befehlszeilenprogramm `aamount` wiederherstellen.

HINWEIS: Dieser Prozess wurde früher als Rollback bezeichnet.

Versuchen Sie dabei nicht, Wiederherstellungspunkte im Ordner „/tmp“ bereitzustellen, da dieser die aavdisk-Dateien enthält.

Die Wiederherstellung von Volumes für geschützte Maschinen ist auch in der AppAssure Core Console möglich. Weitere Informationen finden Sie unter Wiederherstellen von Volumes aus einem Wiederherstellungspunkt.

VORSICHT: Sie sollten nicht versuchen, das System- oder Stamm-Volume (/) wiederherzustellen.

So stellen Sie Volumes einer Linux-Maschine über die Befehlszeile wieder her

1 Führen Sie das AppAssure-Dienstprogramm `aamount` als Root aus, z. B.:

```
sudo aamount
```

2 Geben Sie an der AppAssure-Eingabeaufforderung den folgenden Befehl ein, um die geschützten Maschinen aufzulisten.

```
lm
```

3 Geben Sie die IP-Adresse oder den Hostnamen des AppAssure Core-Servers ein.

4 Geben Sie die Anmeldeinformationen (Benutzername und Kennwort) für den Server ein.

Daraufhin wird eine Liste der vom jeweiligen AppAssure-Server geschützten Maschinen angezeigt. Die Liste enthält die gefundenen Maschinen mit laufender Zeilennummer, Host/IP-Adresse und ID-Nummer für die Maschine (z. B.: 293cc667-44b4-48ab-91d8-44bc74252a4f).

5 Geben Sie den folgenden Befehl ein, um die derzeit bereitgestellten Wiederherstellungspunkte für die angegebene Maschine anzuzeigen:

```
lr <Zeilennummer_der_Maschine>
```

> **HINWEIS:** Sie können in diesem Befehl auch die ID-Nummer der Maschine anstelle der laufenden Zeilennummer angeben.

Daraufhin werden die Basiswiederherstellungspunkte und die inkrementellen Wiederherstellungspunkte für die betreffende Maschine angezeigt. Die Liste umfasst eine laufende Zeilennummer, Datum/Zeitstempel, Speicherort des Volumes, Größe des Wiederherstellungspunkts und eine ID-Nummer für das Volume mit einer laufenden Nummer am Ende (z. B. R293cc667-44b4-48ab-91d8-44bc74252a4f:2“), die den Wiederherstellungspunkt kennzeichnet.

6 Geben Sie den folgenden Befehl ein, um einen Wiederherstellungspunkt für die Wiederherstellung auszuwählen:

```
r <ID-Nummer_für_Volume-Wiederherstellungspunkt> <Pfad>
```

Dieser Befehl stellt das Volume-Image mit der angegebenen ID vom Core im angegebenen Pfad wieder her. Der Pfad für die Wiederherstellung ist der Pfad für den Deskriptor der Gerätedatei und nicht das Bereitstellungsverzeichnis.

> **HINWEIS:** Sie können im Befehl auch die Zeilennummer anstelle der ID-Nummer für den Wiederherstellungspunkt angeben, um den Wiederherstellungspunkt anzugeben. In diesem Fall müssen Sie die Zeilennummer für Agent/Maschine (in der lm-Ausgabe), gefolgt von der Zeilennummer des Wiederherstellungspunkts und dem Volume-Buchstaben und dahinter den Pfad angeben, z. B. „r <Zeilennummer_für_Maschine> <Zeilennummer_für_Wiederherstellungspunkt> <Volume-Buchstabe> <Pfad>“. In diesem Befehl ist <Pfad> der Dateideskriptor für das eigentliche Volume.
>
> Wenn die `lm`-Ausgabe beispielsweise drei Agent-Maschinen auflistet, Sie den Befehl `lr` für Nummer `2` eingeben und das Volume `b` des Wiederherstellungspunkts `23` im Volume wiederherstellen möchten, das im Verzeichnis `/mnt/data` bereitgestellt wurde. lautet der Befehl:
>
> ```
> r2 23 b /mnt/data
> ```
>
> Es ist möglich, eine Wiederherstellung im Stammverzeichnis (/) durchzuführen, allerdings nur mit einer BMR-Wiederherstellung (Bare Metal Restore) mit Start von einer Live DVD. Weitere Informationen finden Sie unter Starten einer BMR-Wiederherstellung für Linux.

7 Geben Sie `y` für Ja ein, wenn Sie aufgefordert werden, den Vorgang fortzusetzen.

Sobald die Wiederherstellung fortgesetzt wird, werden entsprechende Meldungen angezeigt, die Sie über den Status informieren.

8 Bei einer erfolgreichen Wiederherstellung stellt das Dienstprogramm `aamount` automatisch wieder das Kernel-Modul im wiederhergestellten Volume bereit, wenn das Ziel vorher geschützt und bereitgestellt war. Andernfalls müssen Sie das wiederhergestellte Volume auf der lokalen Festplatte bereitstellen (z. B. mit dem Befehl `sudo mount`) und anschließend überprüfen, ob die Dateien wiederhergestellt wurden (z. B. mit dem Befehl `ls`).

Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer

Sie können mit Windows-Explorer Verzeichnisse und Dateien in einem Wiederherstellungspunkt kopieren und auf einer Windows-Maschine einfügen. Dies kann hilfreich sein, wenn nur ein Teil eines Wiederherstellungspunkts Benutzern zur Verfügung gestellt werden soll.

Beim Kopieren von Verzeichnissen und Dateien werden die Zugriffsberechtigungen des Benutzers verwendet, der den Kopiervorgang durchführt, und auf die eingefügten Verzeichnisse und Dateien übernommen. Informationen zum Beibehalten der ursprünglichen Dateiberechtigungen beim Wiederherstellen von Verzeichnissen und Dateien für Benutzer (z. B. beim Wiederherstellen eines Benutzerordners auf einem Dateiserver) finden Sie unter Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer und Beibehalten der Berechtigungen.

So stellen Sie Verzeichnisse oder Dateien mit Windows-Explorer wieder her

1. Stellen Sie den Wiederherstellungspunkt bereit, der die wiederherzustellenden Daten enthält. Entsprechende Details finden Sie unter Bereitstellen eines Wiederherstellungspunktes für eine Windows-Maschine.
2. Navigieren Sie in Windows-Explorer zum bereitgestellten Wiederherstellungspunkt und wählen Sie die Verzeichnisse und Dateien aus, die wiederhergestellt werden sollen. Wählen Sie im Kontextmenü **Kopieren** aus.
3. Navigieren Sie in Windows-Explorer zum Speicherort auf der Maschine, in dem die Daten wiederhergestellt werden sollen. Wählen Sie im Kontextmenü **Einfügen** aus.

Wiederherstellen von Verzeichnissen oder Dateien mit Windows-Explorer und Beibehalten der Berechtigungen

Sie können mit Windows-Explorer Verzeichnisse und Dateien in einem Wiederherstellungspunkt kopieren und auf einer Windows-Maschine einfügen, ohne dass die Dateizugriffsberechtigungen verloren gehen.

Wenn Sie beispielsweise einen Ordner wiederherstellen müssen, der auf einem Dateiserver nur für bestimmte Benutzer zugänglich war, können Sie die Befehle **Kopieren** und **Einfügen mit Berechtigungen** verwenden, um sicherzustellen, dass die eingeschränkten Zugriffsberechtigungen der wiederhergestellten Dateien erhalten bleiben. So kann vermieden werden, dass die Berechtigungen erneut manuell auf die wiederhergestellten Verzeichnisse und Dateien angewendet werden.

HINWEIS: Der Befehl „Einfügen mit Berechtigungen“ ist im AppAssure Core und Agent verfügbar. Es steht im Local Mount Utility nicht zur Verfügung.

So stellen Sie Verzeichnisse oder Dateien mit Windows-Explorer mit Beibehaltung der Berechtigungen wieder her

1. Stellen Sie den Wiederherstellungspunkt bereit, der die wiederherzustellenden Daten enthält. Entsprechende Details finden Sie unter Bereitstellen eines Wiederherstellungspunktes für eine Windows-Maschine.
2. Navigieren Sie in Windows-Explorer zum bereitgestellten Wiederherstellungspunkt und wählen Sie die Verzeichnisse und Dateien aus, die wiederhergestellt werden sollen. Wählen Sie im Kontextmenü **Kopieren** aus.
3. Navigieren Sie in Windows-Explorer zum Speicherort auf der Maschine, in dem die Daten wiederhergestellt werden sollen. Wählen Sie im Kontextmenü **Einfügen mit Berechtigungen** aus.

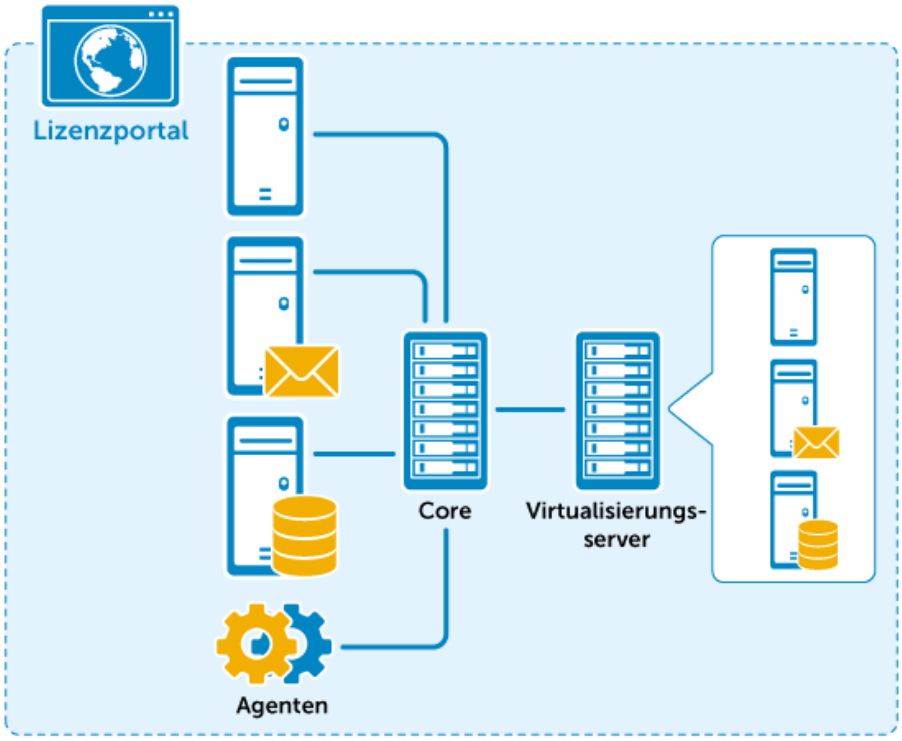
   HINWEIS: Wenn der Befehl **Einfügen mit Berechtigungen** im Kontextmenü deaktiviert ist, sind die Dateien, die kopiert werden sollen, in Windows-Explorer nicht bekannt. Wiederholen Sie Schritt 2, um den Befehl **Einfügen mit Berechtigungen** im Kontextmenü zu aktivieren.

Information zum Exportieren geschützter Daten von Windows-Maschinen in virtuelle Maschinen

AppAssure unterstützt den einmaligen Export sowie den kontinuierlichen Export (Virtual Standby) von Windows-Sicherungsinformationen in eine virtuelle Maschine. Der Export von Daten auf eine Virtual Standby-Maschine stellt eine Datenkopie mit hoher Verfügbarkeit bereit. Sollte eine geschützte Maschine ausfallen, können Sie die virtuelle Maschine starten und anschließend die Wiederherstellung durchführen.

Das folgende Diagramm veranschaulicht eine typische Implementierung für den Export von Daten in eine virtuelle Maschine.

Abbildung 8. Virtual Standby-Implementierung



Beim Export in eine virtuelle Maschine werden alle Sicherungsdaten eines Wiederherstellungspunkts sowie die für den Schutzzeitplan der Maschine definierten Parameter exportiert. So können Sie ein virtuelles Standby erreichen, da die geschützten Daten laufend von der geschützten Maschine in eine virtuelle Maschine exportiert werden.

Sie können einen virtuellen Export von Wiederherstellungspunkten für geschützte Windows- oder Linux-Agent-Maschinen nach VMware, ESXi, Hyper-V und VirtualBox durchführen.

HINWEIS: Bei ESXi, VMware Workstation oder Hyper-V muss die Version der virtuellen Maschine eine lizenzierte Version der jeweiligen virtuellen Maschinen sein. Testversionen oder Evaluierungsversionen werden nicht unterstützt.

Wenn zwischen zwei Cores (Quelle und Ziel) eine Replikation eingerichtet ist, können Sie nur Daten von Ziel-Core exportieren, nachdem die Anfangsreplikation durchgeführt wurde.

Verwalten von Exporten

Virtual Standby ist ein P2V-Prozess (physisch-zu-virtuell), bei dem eine virtuelle Maschine (Klon) einer geschützten Maschine oder eines Agenten erstellt wird. Ein Virtual Standby kann mithilfe eines Ad-hoc-Exportvorgangs oder eines Exportvorgangs mit laufender Aktualisierung erstellt werden. Bei einem Virtual Standby mit laufender Aktualisierung wird er nach jedem vom Quellagenten erfassten Snapshot eine inkrementelle Aktualisierung durchgeführt.

HINWEIS: AppAssure unterstützt Hyper-V-Exporte nach Windows 8, Windows 8.1, Windows Server 2012 und 2012 R2.

Auf der Registerkarte „Virtual Standby“ in der Core Console können Sie den Status der Exportvorgänge anzeigen, die derzeit eingerichtet sind. Dies umfasst einmalige Exporte und kontinuierliche Exporte für Virtual Standby. Auf dieser Registerkarte können Sie unterschiedliche Verwaltungsaufgaben für Exporte durchführen,

z. B. Exportvorgänge vorübergehend deaktivieren, beenden oder entfernen. Sie können auch eine Warteschlange der bevorstehenden Exportvorgänge anzeigen.

So verwalten Sie Exporte

1 Navigieren Sie in der Core Console zur Registerkarte „Virtual Standby“.

Auf der Registerkarte „Virtual Standby“ wird eine Tabelle mit den gespeicherten Exporteinstellungen angezeigt (siehe Beschreibung in der folgenden Tabelle).

Tabelle 69.

Spalte	Beschreibung
Status	Der Status der Virtual Standby-Konfiguration, angezeigt als Symbol. Die folgenden Statussymbole können angezeigt werden: • Grünes Symbol: Virtual Standby wurde erfolgreich konfiguriert, ist aktiv und wurde nicht vorübergehend deaktiviert. Der nächste Virtual Standby-Export wird unmittelbar nach dem nächsten Snapshot durchgeführt. • Gelbes Symbol: Virtual Standby wurde vorübergehend deaktiviert, wird aber weiterhin vom Core gespeichert. Nach einer neuen Übertragung wird der Exportjob allerdings nicht automatisch gestartet, sodass keine neuen Virtual Standby-Exporte für den betreffenden Agenten durchgeführt werden.
Name der Maschine	Der Name der Quellmaschine.
Ziel	Die virtuelle Maschine und der Pfad, in den die Daten exportiert werden.
Exporttyp	Der Typ der virtuellen Maschinenplattform für den Export, z. B. ESXi, VMware, Hyper-V oder VirtualBox.
Letzter Export	Datum und Uhrzeit des letzten Exportvorgangs. Wenn soeben ein Export hinzugefügt, aber nicht abgeschlossen wurde, wird eine Meldung mit dem Hinweis angezeigt, dass der Export noch nicht durchgeführt wurde. Wenn ein Export fehlgeschlagen ist oder abgebrochen wurde, wird ebenfalls eine entsprechende Meldung angezeigt.

2 Wählen Sie einen Export aus, wenn Sie die gespeicherten Exporteinstellungen verwalten möchten, und klicken Sie dann auf eine der folgenden Optionen:

- **Vorübergehend deaktivieren**: Der Export wird vorübergehend deaktiviert.
- **Wieder aktivieren**: Ein vorübergehend deaktivierter Export wird fortgesetzt.
- **Erzwingen**: Es wird ein neuer Export erstellt. Diese Option kann hilfreich sein, wenn Virtual Standby vorübergehend deaktiviert und wieder aktiviert wurde, da der Exportjob erst nach einer neuen Übertragung wieder gestartet wird. Sie können dann einen Export erzwingen, wenn Sie nicht auf die neue Übertragung warten möchten.

3 Klicken Sie auf **Entfernen**, um einen Export aus dem System zu entfernen. Wenn Sie einen Export entfernen, wird der Export permanent aus dem System entfernt und kann nicht erneut gestartet werden.

4 Klicken Sie auf **Exportwarteschlange einblenden**, um Details zu den aktiven Exportvorgängen anzuzeigen, die derzeit in der Warteschlange sind.

Die Tabelle „Exportwarteschlange“ wird unter der Tabelle „Virtual Standby“ angezeigt und enthält die in der folgenden Tabelle beschriebenen Informationen.

Tabelle 70.

Spalte	Beschreibung
Name der Maschine	Der Name der Quellmaschine.
Ziel	Die virtuelle Maschine und der Pfad, in den die Daten exportiert werden.

Tabelle 70.

Spalte	Beschreibung
Exporttyp	Der Typ der virtuellen Maschinenplattform für den Export, z. B. ESXi, VMware, Hyper-V oder VirtualBox.
Zeitplantyp	Der Typ des Exports („Einmalig“ oder „Kontinuierlich“).
Status	Der Exportfortschritt, angezeigt als Prozentwert in einer Fortschrittsanzeige.

5 Gehen Sie folgendermaßen vor, um die Anzahl der Exportvorgänge festzulegen, die gleichzeitig durchgeführt werden können:

- Klicken Sie in der Tabelle „Exportwarteschlange“ auf **Maximale Anzahl gleichzeitiger Exportvorgänge**.
- Geben Sie im Dialogfeld „Maximale Anzahl gleichzeitiger Exportvorgänge“ eine Zahl ein und klicken Sie auf **Speichern**. Die Standardeinstellung ist 5.

6 Um einen Exportvorgang in der Exportwarteschlange abzubrechen, wählen Sie den Export in der Tabelle „Exportwarteschlange“ aus und klicken Sie dann auf **Abbrechen**.

7 Um einen neuen Virtual Standby-Export hinzuzufügen, können Sie auf **Hinzufügen** klicken, um den Exportassistenten zu starten. Weitere Informationen zum Einrichten von Virtual Standby für eine bestimmte virtuelle Maschine finden Sie in den folgenden Abschnitten:

- Durchführen eines kontinuierlichen ESXi-Exports (Virtual Standby)
- Durchführen eines kontinuierlichen VMware Workstation-Exports (Virtual Standby)
- Durchführen eines kontinuierlichen Hyper-V-Exports (Virtual Standby)
- Durchführen eines kontinuierlichen VirtualBox-Exports (Virtual Standby)
- Exportieren von Sicherungsinformationen aus einer Linux-Maschine in eine virtuelle Maschine

Exportieren von Daten aus einer Windows-Maschine in eine virtuelle Maschine

In AppAssure können Sie Daten von Windows-Maschinen in eine virtuelle Maschine (VMware, ESXi, Hyper-V und VirtualBox) exportieren, indem Sie alle Sicherungsinformationen aus einem Wiederherstellungspunkt sowie die für den Schutzzeitplan für Ihre Maschine definierten Parameter exportieren.

So exportieren Sie Windows-Sicherungsinformationen in eine virtuelle Maschine

- Navigieren Sie in der AppAssure Core Console zu der Maschine, die Sie exportieren möchten. Klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü **Aktionen** auf **Export** und wählen Sie dann den gewünschten Exporttyp aus („Einmalig“ oder „Virtual Standby“). Der Exportassistent wird angezeigt.

  Weitere Informationen zum Exportieren von Windows-Daten in einen bestimmte virtuelle Maschine finden Sie in den folgenden Abschnittet.

  - Exportieren von Windows-Daten mit ESXi-Export
  - Exportieren von Windows-Daten mit VMware Workstation-Export
  - Exportieren von Windows-Daten mit Hyper-V-Export
  - Exportieren von Windows-Daten nach VirtualBox

Exportieren von Windows-Daten mit ESXi-Export

In AppAssure können Sie Daten nach ESXi exportieren, indem Sie einen einmaligen Export durchführen oder einen kontinuierlichen Export (Virtual Standby) einrichten. Führen Sie die nachstehend aufgeführten Schritte für den jeweiligen Exporttyp aus.

Durchführen eines einmaligen ESXi-Exports

Führen Sie die folgenden Schritte aus, um einen einmaligen ESXi-Export durchzuführen.

So führen Sie einen einmaligen ESXi-Export durch

1 Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:

- Klicken Sie in der Schaltflächenleiste auf **Export**, um den Exportassistenten zu starten, und führen Sie dann die folgenden Schritte aus:
  - a Wählen Sie auf der Seite „Exporttyp auswählen“ **Einmaliger Export** aus und klicken Sie dann auf **Weiter**.
  - b Wählen Sie auf der Seite „Geschützte Maschinen“ die geschützte Maschine aus, die Sie in eine virtuelle Maschine exportieren möchten, und klicken Sie dann auf **Weiter**.
- Navigieren Sie zu der Maschine, die exportiert werden soll, und wählen Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü „Aktionen“ der betreffenden Maschine **Export** > **Einmalig** aus.

  Im Exportassistenten wird die Seite „Wiederherstellungspunkte“ angezeigt.

2 Wählen Sie auf der Seite „Wiederherstellungspunkte“ den Wiederherstellungspunkt des AppAssure 5 Core aus, den Sie exportieren möchten, und klicken Sie dann auf **Weiter**.

Definieren von Informationen für virtuelle Maschinen zum Durchführen eines ESXi-Exports

Führen Sie die folgenden Schritte aus, um die Informationen für die virtuelle Maschine zu definieren.

So definieren Sie Informationen für virtuelle Maschinen zum Durchführen eines ESXi-Exports

1 Wählen Sie auf der Seite „Ziel“ des Exportassistenten im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ **ESX(i)** aus.

2 Geben Sie die Parameter für den Zugriff auf die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle), und klicken Sie auf **Weiter**.

Tabelle 71.

Optionen	Beschreibung
Hostname	Geben Sie einen Namen für die Hostmaschine ein.
Port	Geben Sie den Port für die Hostmaschine ein. Die Standardeinstellung ist 443.
Benutzername	Geben Sie die Anmeldeinformationen für die Hostmaschine ein.
Kennwort	Geben Sie die Anmeldeinformationen für die Hostmaschine ein.

3 Geben Sie auf der Seite „Optionen für virtuelle Maschine“ die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 72.

Option	Beschreibung
Ressourcenpool	Wählen Sie einen Ressourcenpool in der Dropdown-Liste aus.
Datenspeicher	Wählen Sie einen Datenspeicher in der Dropdown-Liste aus.

Tabelle 72.

Option	Beschreibung
Name der virtuellen Maschine	Geben Sie einen Namen für die virtuelle Maschine ein.
Arbeitsspeicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • **Gleiche RAM-Größe verwenden wie Quellmaschine** • **„Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben** Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.
Datenträgerbereitstellung	Wählen Sie den Typ der Datenträgerbereitstellung aus („Thin“ oder „Thick“).
Datenträgerzuordnung	Geben Sie den Typ der Datenträgerzuordnung an („Automatisch“ oder „Manuell“).
Version	Wählen Sie die Version der virtuellen Maschine aus.

4 Klicken Sie auf **Weiter**.

5 Wählen Sie auf der Seite „Volumes“ die Volumes aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.

6 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

HINWEIS: Sie können den Status und Fortschritt des Exports auf der Registerkarte „Virtual Standby“ oder auf der Registerkarte „Ereignisse“ überwachen.

Durchführen eines kontinuierlichen ESXi-Exports (Virtual Standby)

Führen Sie die folgenden Schritte aus, um einen kontinuierlichen ESXi-Export durchzuführen.

So führen Sie einen kontinuierlichen ESXi-Export (Virtual Standby) durch

1 Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:

- Klicken Sie auf der Registerkarte „Virtual Standby“ auf **Hinzufügen** klicken, um den Exportassistenten zu starten. Wählen Sie auf der Seite „Geschützte Maschinen“ des Exportassistenten die geschützte Maschine aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.
- Navigieren Sie zu der Maschine, die exportiert werden soll, und klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü „Aktionen“ der betreffenden Maschine auf **Export** > **Virtual Standby**.

2 Wählen Sie auf der Seite „Ziel“ des Exportassistenten im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ **ESXi** aus.

3 Geben Sie die Informationen für den Zugriff auf die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle), und klicken Sie auf **Weiter**.

Tabelle 73.

Option	Beschreibung
Hostname	Geben Sie einen Namen für die Hostmaschine ein.
Port	Geben Sie den Port für die Hostmaschine ein. Die Standardeinstellung ist 443.

Tabelle 73.

Option	Beschreibung
Benutzername	Geben Sie die Anmeldeinformationen für die Hostmaschine ein.
Kennwort	Geben Sie die Anmeldeinformationen für die Hostmaschine ein.

4 Geben Sie auf der Seite „Optionen für virtuelle Maschine“ die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 74.

Option	Beschreibung
Ressourcenpool	Wählen Sie einen Ressourcenpool in der Dropdown-Liste aus.
Datenspeicher	Wählen Sie einen Datenspeicher in der Dropdown-Liste aus.
Name der virtuellen Maschine	Geben Sie einen Namen für die virtuelle Maschine ein.
Arbeitsspeicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • **Gleiche RAM-Größe verwenden wie Quellmaschine** • **„Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben** Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.
Datenträgerbereitstellung	Wählen Sie den Typ der Datenträgerbereitstellung aus („Thin“ oder „Thick“).
Datenträgerzuordnung	Geben Sie den Typ der Datenträgerzuordnung an („Automatisch“, „Manuell“ oder „Mit VM“).
Version	Wählen Sie die Version der virtuellen Maschine aus.
Ersten Ad-Hoc-Export durchführen	Wählen Sie diese Option aus, um den virtuellen Export sofort und nicht nach dem nächsten geplanten Snapshot durchzuführen.

5 Klicken Sie auf **Weiter**.

6 Wählen Sie auf der Seite „Volumes“ die Volumes aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.

7 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

ⓘ **HINWEIS:** Sie können den Status und Fortschritt des Exports auf der Registerkarte „Virtual Standby“ oder auf der Registerkarte „Ereignisse“ überwachen.

Exportieren von Windows-Daten mit VMware Workstation-Export

In AppAssure können Sie Daten nach VMware Workstation exportieren, indem Sie einen einmaligen Export durchführen oder einen kontinuierlichen Export (Virtual Standby) einrichten. Führen Sie die nachstehend aufgeführten Schritte für den jeweiligen Exporttyp aus.

Durchführen eines einmaligen VMware Workstation-Exports

Führen Sie die folgenden Schritte aus, um einen einmaligen VMware Workstation-Export durchzuführen.

So führen Sie einen einmaligen VMware Workstation-Export durch

1 Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:

- Klicken Sie in der Schaltflächenleiste auf **Export**, um den Exportassistenten zu starten, und führen Sie dann die folgenden Schritte aus:
  a Wählen Sie auf der Seite „Exporttyp auswählen“ **Einmaliger Export** aus und klicken Sie dann auf **Weiter**.
  b Wählen Sie auf der Seite „Geschützte Maschinen“ die geschützte Maschine aus, die Sie in eine virtuelle Maschine exportieren möchten, und klicken Sie dann auf **Weiter**.
- Navigieren Sie zu der Maschine, die exportiert werden soll, und wählen Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü „Aktionen“ der betreffenden Maschine **Export** > **Einmalig** aus.

  Im Exportassistenten wird die Seite „Wiederherstellungspunkte“ angezeigt.

2 Wählen Sie auf der Seite „Wiederherstellungspunkte“ den Wiederherstellungspunkt des AppAssure 5 Core aus, den Sie exportieren möchten, und klicken Sie dann auf **Weiter**.

Definieren von Einstellungen zum Durchführen eines einmaligen VMware Workstation-Exports

Führen Sie die folgenden Schritte aus, um die Einstellungen zum Durchführen eines einmaligen VMware Workstation-Exports zu definieren.

So definieren Sie die Einstellungen zum Durchführen eines einmaligen VMware Workstation-Exports

1 Wählen Sie auf der Seite „Ziel“ des Exportassistenten im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ **VMware Workstation** aus und klicken Sie auf **Weiter**.

2 Geben Sie auf der Seite „Optionen für virtuelle Maschine“ die in der folgenden Tabelle beschriebenen Parameter für den Zugriff auf die virtuelle Maschine ein.

Tabelle 75.

Option	Beschreibung
Speicherort	Geben Sie den Pfad des lokalen Ordners oder die Netzwerkfreigabe für die Erstellung der virtuellen Maschine an. **HINWEIS:** Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie gültige Anmeldeinformationen für ein Konto eingeben, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen für die Netzwerkfreigabe verfügen.
Benutzername	Geben Sie die Anmeldeinformationen für den Netzwerkspeicherort für den Export ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie einen gültigen Benutzernamen für ein Konto eingeben, das auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Benutzername erforderlich.

Tabelle 75.

Option	Beschreibung
Kennwort	Geben Sie die Anmeldeinformationen für den Netzwerkspeicherort für den Export ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie ein gültiges Kennwort für ein Konto eingeben, das auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Kennwort erforderlich.
Name der virtuellen Maschine	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein, z. B. VM-0A1B2C3D4. **HINWEIS:** Standardmäßig wird der Name der Quellmaschine verwendet.
Version	Wählen Sie die VMware Workstation-Version der virtuellen Maschine aus. Sie haben folgende Auswahlmöglichkeiten: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0
Arbeitsspeicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • **Gleiche RAM-Größe verwenden wie Quellmaschine** • **„Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben** Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.

3 Klicken Sie auf **Weiter**.

4 Wählen Sie auf der Seite „Volumes“ die Volumes aus, die Sie exportieren möchten, z. B. C:\ und D:\, und klicken Sie dann auf **Weiter**.

5 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

HINWEIS: Sie können den Status und Fortschritt des Exports auf der Registerkarte „Virtual Standby“ oder auf der Registerkarte „Ereignisse“ überwachen.

Durchführen eines kontinuierlichen VMware Workstation-Exports (Virtual Standby)

Führen Sie die folgenden Schritte aus, um einen kontinuierlichen VMware Workstation-Export durchzuführen.

So führen Sie einen kontinuierlichen VMware Workstation-Export (Virtual Standby) durch

1 Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:

- Klicken Sie auf der Registerkarte „Virtual Standby“ auf **Hinzufügen** klicken, um den Exportassistenten zu starten. Wählen Sie auf der Seite „Geschützte Maschinen“ des Exportassistenten die geschützte Maschine aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.
- Navigieren Sie zu der Maschine, die exportiert werden soll, und klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü „Aktionen“ der betreffenden Maschine auf **Export** > **Virtual Standby**.

2 Wählen Sie auf der Seite „Ziel“ des Exportassistenten im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ **VMware Workstation** aus und klicken Sie auf **Weiter**.

3 Geben Sie auf der Seite „Optionen für virtuelle Maschine“ die in der folgenden Tabelle beschriebenen Parameter für den Zugriff auf die virtuelle Maschine ein.

Tabelle 76.

Option	Beschreibung
Zielpfad	Geben Sie den Pfad des lokalen Ordners oder die Netzwerkfreigabe für die Erstellung der virtuellen Maschine an. **HINWEIS:** Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie gültige Anmeldeinformationen für ein Konto eingeben, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen für die Netzwerkfreigabe verfügen.
Benutzername	Geben Sie die Anmeldeinformationen für den Netzwerkspeicherort für den Export ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie einen gültigen Benutzernamen für ein Konto eingeben, das auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Benutzername erforderlich.
Kennwort	Geben Sie die Anmeldeinformationen für den Netzwerkspeicherort für den Export ein. • Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie ein gültiges Kennwort für ein Konto eingeben, das auf der Zielmaschine registriert ist. • Wenn Sie einen lokalen Pfad angegeben haben, ist kein Kennwort erforderlich.
Virtuelle Maschine	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein, z. B. VM-0A1B2C3D4. **HINWEIS:** Standardmäßig wird der Name der Quellmaschine verwendet.
Version	Wählen Sie die VMware Workstation-Version der virtuellen Maschine aus. Sie haben folgende Auswahlmöglichkeiten: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0
Arbeitsspeicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • **Gleiche RAM-Größe verwenden wie Quellmaschine** • **„Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben** Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.

4 Wählen Sie **Ersten Ad-Hoc-Export durchführen**, um den virtuellen Export sofort und nicht nach dem nächsten geplanten Snapshot durchzuführen.

5 Klicken Sie auf **Weiter**.

6 Wählen Sie auf der Seite „Volumes“ die Volumes aus, die Sie exportieren möchten, z. B. C:\ und D:\, und klicken Sie dann auf **Weiter**.

7 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

HINWEIS: Sie können den Status und Fortschritt des Exports auf der Registerkarte „Virtual Standby“ oder auf der Registerkarte „Ereignisse“ überwachen.

Exportieren von Windows-Daten mit Hyper-V-Export

In AppAssure können Sie Daten mit einem Hyper-V-Export exportieren, indem Sie einen einmaligen Export durchführen oder einen kontinuierlichen Export (Virtual Standby) einrichten.

AppAssure 5 unterstützt einen Hyper-V-Export der ersten Generation auf die folgenden Hosts:

- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

AppAssure 5 unterstützt einen Hyper-V-Export der zweiten Generation auf die folgenden Hosts:

- Windows 8.1
- Windows Server 2012 R2

HINWEIS: Nicht alle geschützten Maschinen können auf Hyper-V-Hosts der zweiten Generation exportiert werden.

Lediglich geschützte Maschinen mit den folgenden UEFI-Betriebssystemen (Unified Extensible Firmware Interface) unterstützen einen Export auf Hyper-V-Hosts der zweiten Generation:

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012R2 (UEFI)

HINWEIS: Der Hyper-V-Export in eine VM der zweiten Generation kann fehlschlagen, wenn auf dem Hyper-V-Host nicht genügend RAM für die Durchführung des Exports zugewiesen wurde.

Führen Sie die nachstehend aufgeführten Schritte für den jeweiligen Exporttyp aus.

Durchführen eines einmaligen Hyper-V-Exports

Führen Sie die folgenden Schritte aus, um einen einmaligen Hyper-V-Export durchzuführen.

So führen Sie einen einmaligen Hyper-V-Export durch

1 Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:

- Klicken Sie in der Schaltflächenleiste auf **Export**, um den Exportassistenten zu starten, und führen Sie dann die folgenden Schritte aus:
  - a Wählen Sie auf der Seite „Exporttyp auswählen“ **Einmaliger Export** aus und klicken Sie dann auf **Weiter**.
  - b Wählen Sie auf der Seite „Geschützte Maschinen“ die geschützte Maschine aus, die Sie in eine virtuelle Maschine exportieren möchten, und klicken Sie dann auf **Weiter**.
- Navigieren Sie zu der Maschine, die exportiert werden soll, und wählen Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü „Aktionen“ der betreffenden Maschine **Export** > **Einmalig** aus.

  Im Exportassistenten wird die Seite „Wiederherstellungspunkte“ angezeigt.

2 Wählen Sie auf der Seite „Wiederherstellungspunkte“ den Wiederherstellungspunkt des AppAssure 5 Core aus, den Sie exportieren möchten, und klicken Sie dann auf **Weiter**.

Definieren von Einstellungen zum Durchführen eines einmaligen Hyper-V-Exports

Führen Sie die folgenden Schritte aus, um die Einstellungen zum Durchführen eines einmaligen Hyper-V-Exports zu definieren.

So definieren Sie die Einstellungen zum Durchführen eines einmaligen Hyper-V-Exports

1 Wählen Sie auf der Seite „Ziel“ des Exportassistenten im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ **Hyper-V** aus.

2 Klicken Sie auf **Lokale Maschine verwenden**, um den Export in eine lokale Maschine durchzuführen, der die Hyper-V-Rolle zugewiesen ist.

3 Klicken Sie auf die Option **Remote-Host**, um anzugeben, dass sich der Hyper-V-Server auf einer Remote-Maschine befindet, und geben Sie dann die in der folgenden Tabelle beschriebenen Informationen für den Remote-Host ein.

Tabelle 77.

Textfeld	Beschreibung
Hostname	Geben Sie eine IP-Adresse oder einen Hostnamen für den Hyper-V-Server ein. Dabei handelt es sich um die IP-Adresse oder den Hostnamen des Remote-Hyper-V-Servers.
Port	Geben Sie eine Portnummer für die Maschine ein. Dabei handelt es sich um den Port, über den der Core mit der Maschine kommuniziert.
Benutzername	Geben Sie den Benutzernamen für den Benutzer mit Administratorberechtigungen für die Workstation mit dem Hyper-V-Server ein. Diese Angabe dient zur Festlegung der Anmeldeinformationen für die virtuelle Maschine.
Kennwort	Geben Sie das Kennwort für das Benutzerkonto mit den Administratorberechtigungen auf der Workstation mit Hyper-V-Server an. Diese Angabe dient zur Festlegung der Anmeldeinformationen für die virtuelle Maschine.

4 Klicken Sie auf **Weiter**.

5 Geben Sie auf der Seite „Optionen für virtuelle Maschine“ im Textfeld „Speicherort für virtuelle Maschine“ den Pfad für die virtuelle Maschine ein, z. B. D:\export. Er wird verwendet, um den Speicherort der virtuellen Maschine anzugeben.

> **HINWEIS:** Sie müssen den Speicherort der virtuellen Maschine für lokale sowie für Remote-Hyper-V-Server angeben. Der Pfad muss ein gültiger lokaler Pfad für den Hyper-V-Server sein. Nicht vorhandene Verzeichnisse werden automatisch erstellt. Sie sollten nicht versuchen, sie manuell zu erstellen. Ein Export in freigegebene Ordner, z. B. \\data\share, ist nicht zulässig.

6 Geben Sie den Namen für die virtuelle Maschine im Textfeld **Name der virtuellen Maschine** ein.

Der Name, den Sie eingeben, wird in der Liste der virtuellen Maschinen in der Hyper-V-Manager-Konsole angezeigt.

7 Geben Sie den Arbeitsspeicher an. Sie haben folgende Auswahlmöglichkeiten:

- **Gleiche RAM-Größe verwenden wie Quellmaschine**: Die RAM-Konfiguration der virtuellen Maschine ist mit der Konfiguration der Quellmaschine identisch.
- **„Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben**

  Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.

8 Klicken Sie zum Angeben der Datenträgerformats neben „Datenträgerformat“ auf eine der folgenden Optionen:

- **VHDX**
- **VHD**

> **HINWEIS:** Der Hyper-V-Export unterstützt VHDX-Datenträgerformate, wenn auf der Zielmaschine Windows 8 (Windows Server 2012) oder höher ausgeführt wird. Wenn VHDX für die jeweilige Umgebung nicht unterstützt wird, ist die Option deaktiviert.
>
> Bei einem Export nach Hyper-V der 2. Generation wird nur das VHDX-Datenträgerformat unterstützt.

9 Klicken Sie auf eine der folgenden Optionen, um die Generation von Hyper-V anzugeben, die für den Export verwendet werden soll:

- Generation 1
- Generation 2

> **HINWEIS:** Nur die 2. Generation unterstützt die Option „Sicherer Start“.

10 Geben Sie den gewünschten Netzwerkadapter für die exportierte VM an.

11 Wählen Sie auf der Seite „Volumes“ die Volumes aus, die Sie exportieren möchten, z. B. C:\.

> **HINWEIS:** Wenn die ausgewählten Volumes größer sind als die maximal zulässige Größe, die von der Anwendung unterstützt wird, oder den verfügbaren Speicherplatz überschreiten, wird eine Fehlermeldung angezeigt.

- Beim VHDX-Datenträgerformat dürfen die ausgewählten Volumes nicht größer als 64 TB sein.
- Beim VHD-Datenträgerformat dürfen die ausgewählten Volumes nicht größer als 2040 GB sein.

12 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

> **HINWEIS:** Sie können den Status und Fortschritt des Exports auf der Registerkarte „Virtual Standby“ oder auf der Registerkarte „Ereignisse“ überwachen.

Durchführen eines kontinuierlichen Hyper-V-Exports (Virtual Standby)

Führen Sie die folgenden Schritte aus, um einen kontinuierlichen Hyper-V-Export durchzuführen.

So führen Sie einen kontinuierlichen Hyper-V-Export (Virtual Standby) durch

1 Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:

- Klicken Sie auf der Registerkarte „Virtual Standby“ auf **Hinzufügen** klicken, um den Exportassistenten zu starten. Wählen Sie auf der Seite „Geschützte Maschinen“ des Exportassistenten die geschützte Maschine aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.
- Navigieren Sie zu der Maschine, die exportiert werden soll, und klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü „Aktionen“ der betreffenden Maschine auf **Export** > **Virtual Standby**.

2 Klicken Sie auf **Lokale Maschine verwenden**, um den Export in eine lokale Maschine durchzuführen, der die Hyper-V-Rolle zugewiesen ist.

3 Klicken Sie auf die Option **Remote-Host**, um anzugeben, dass sich der Hyper-V-Server auf einer Remote-Maschine befindet, und geben Sie dann die in der folgenden Tabelle beschriebenen Parameter für den Remote-Host ein.

Tabelle 78.

Textfeld	Beschreibung
Hostname	Geben Sie eine IP-Adresse oder einen Hostnamen für den Hyper-V-Server ein. Dabei handelt es sich um die IP-Adresse oder den Hostnamen des Remote-Hyper-V-Servers.
Port	Geben Sie eine Portnummer für die Maschine ein. Dabei handelt es sich um den Port, über den der Core mit der Maschine kommuniziert.
Benutzername	Geben Sie den Benutzernamen für den Benutzer mit Administratorberechtigungen für die Workstation mit dem Hyper-V-Server ein. Diese Angabe dient zur Festlegung der Anmeldeinformationen für die virtuelle Maschine.
Kennwort	Geben Sie das Kennwort für das Benutzerkonto mit den Administratorberechtigungen auf der Workstation mit Hyper-V-Server an. Diese Angabe dient zur Festlegung der Anmeldeinformationen für die virtuelle Maschine.

4 Klicken Sie auf **Weiter**.

5 Geben Sie auf der Seite „Optionen für virtuelle Maschine“ im Textfeld „Speicherort für virtuelle Maschine“ den Pfad für die virtuelle Maschine ein, z. B. D:\export. Er wird verwendet, um den Speicherort der virtuellen Maschine anzugeben.

> **HINWEIS:** Sie müssen den Speicherort der virtuellen Maschine für lokale sowie für Remote-Hyper-V-Server angeben. Der Pfad muss ein gültiger lokaler Pfad für den Hyper-V-Server sein. Nicht vorhandene Verzeichnisse werden automatisch erstellt. Sie sollten nicht versuchen, sie manuell zu erstellen. Ein Export in freigegebene Ordner, z. B. \\data\share, ist nicht zulässig.

6 Geben Sie den Namen für die virtuelle Maschine im Textfeld **Name der virtuellen Maschine** ein.

Der Name, den Sie eingeben, wird in der Liste der virtuellen Maschinen in der Hyper-V-Manager-Konsole angezeigt.

7 Geben Sie den Arbeitsspeicher an. Sie haben folgende Auswahlmöglichkeiten:

- **Gleiche RAM-Größe verwenden wie Quellmaschine**: Die RAM-Konfiguration der virtuellen Maschine ist mit der Konfiguration der Quellmaschine identisch.
- **„Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben**

  Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.

8 Klicken Sie zum Angeben der Datenträgerformats neben „Datenträgerformat“ auf eine der folgenden Optionen:

- **VHDX**
- **VHD**

> **HINWEIS:** Der Hyper-V-Export unterstützt VHDX-Datenträgerformate, wenn auf der Zielmaschine Windows 8 (Windows Server 2012) oder höher ausgeführt wird. Wenn VHDX für die jeweilige Umgebung nicht unterstützt wird, ist die Option deaktiviert.
>
> Bei einem Export nach Hyper-V der 2. Generation wird nur das VHDX-Datenträgerformat unterstützt.

9 Klicken Sie auf eine der folgenden Optionen, um die Generation von Hyper-V anzugeben, die für den Export verwendet werden soll:

- Generation 1
- Generation 2

> **HINWEIS:** Nur die 2. Generation unterstützt die Option „Sicherer Start“.

10 Geben Sie den gewünschten Netzwerkadapter für die exportierte VM an.

11 Wählen Sie auf der Seite „Volumes“ die Volumes aus, die Sie exportieren möchten, z. B. C:\.

> **HINWEIS:** Wenn die ausgewählten Volumes größer sind als die maximal zulässige Größe, die von der Anwendung unterstützt wird, oder den verfügbaren Speicherplatz überschreiten, wird eine Fehlermeldung angezeigt.

- Beim VHDX-Datenträgerformat dürfen die ausgewählten Volumes nicht größer als 64 TB sein.
- Beim VHD-Datenträgerformat dürfen die ausgewählten Volumes nicht größer als 2040 GB sein.

12 Wählen Sie **Ersten Ad-Hoc-Export durchführen**, um den virtuellen Export sofort und nicht nach dem nächsten geplanten Snapshot durchzuführen.

13 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

> **HINWEIS:** Sie können den Status und Fortschritt des Exports auf der Registerkarte „Virtual Standby“ oder auf der Registerkarte „Ereignisse“ überwachen.

Exportieren von Windows-Daten nach VirtualBox

In AppAssure können Sie Daten mit einem VirtualBox-Export exportieren, indem Sie einen einmaligen Export durchführen oder einen kontinuierlichen Export (Virtual Standby) einrichten. Führen Sie die nachstehend aufgeführten Schritte für den jeweiligen Exporttyp aus.

> **HINWEIS:** Um einen derartigen Export durchführen zu können, muss VirtualBox auf der Core-Maschine installiert sein. Für Windows-Hosts wird VirtualBox, Version 4.2.18 oder höher unterstützt.

Durchführen eines einmaligen VirtualBox-Exports

Führen Sie die folgenden Schritte aus, um einen einmaligen VirtualBox-Export durchzuführen.

So führen Sie einen einmaligen VirtualBox-Export durch

1 Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:

- Klicken Sie in der Schaltflächenleiste auf **Export**, um den Exportassistenten zu starten, und führen Sie dann die folgenden Schritte aus:
  a Wählen Sie auf der Seite „Exporttyp auswählen“ **Einmaliger Export** aus und klicken Sie dann auf **Weiter**.
  b Wählen Sie auf der Seite „Geschützte Maschinen“ die geschützte Maschine aus, die Sie in eine virtuelle Maschine exportieren möchten, und klicken Sie dann auf **Weiter**.
- Navigieren Sie zu der Maschine, die exportiert werden soll, und wählen Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü „Aktionen“ der betreffenden Maschine **Export** > **Einmalig** aus.

  Im Exportassistenten wird die Seite „Wiederherstellungspunkte“ angezeigt.

2 Wählen Sie auf der Seite „Wiederherstellungspunkte“ den Wiederherstellungspunkt des AppAssure 5 Core aus, den Sie exportieren möchten, und klicken Sie dann auf **Weiter**.

3 Wählen Sie auf der Seite „Ziel“ des Exportassistenten im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ **VirtualBox** aus und klicken Sie auf **Weiter**.

4 Wählen Sie auf der Seite „Optionen für virtuelle Maschine“ **Windows-Maschine verwenden** aus.

5 Geben Sie die Parameter für den Zugriff auf die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 79.

Option	Beschreibung
Name der virtuellen Maschine	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein. **HINWEIS:** Standardmäßig wird der Name der Quellmaschine verwendet.
Zielpfad	Geben Sie einen lokalen oder Remote-Zielpfad für die Erstellung der virtuellen Maschine an. **HINWEIS:** Der Zielpfad darf kein Stammverzeichnis sein. Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie gültige Anmeldeinformationen (Benutzername und Konto) für ein Konto eingeben, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen für die Netzwerkfreigabe verfügen.
Arbeitsspeicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • **Gleiche RAM-Größe verwenden wie Quellmaschine** • **„Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben** Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.

6 Wählen Sie **Benutzerkonto für die exportierte virtuelle Maschine angeben** aus, um ein Benutzerkonto für die virtuelle Maschine anzugeben, und geben Sie die folgenden Informationen ein. Hierbei handelt es sich um ein bestimmtes Benutzerkonto, für das die virtuelle Maschine registriert wird, falls auf der virtuellen Maschine mehrere Benutzerkonten vorhanden sind. Nur der Benutzer, der sich mit diesem Benutzerkonto anmeldet, kann die betreffende virtuelle Maschine im VirtualBox-Manager sehen. Wird kein Konto angegeben, wird die virtuelle Maschine für alle vorhandenen Benutzer auf der Windows-Maschine mit VirtualBox registriert.

- **Benutzername**: Geben Sie den Benutzernamen ein, für den die virtuelle Maschine registriert wird.
- **Kennwort**: Geben Sie das Kennwort für dieses Konto ein.

7 Klicken Sie auf **Weiter**.

8 Wählen Sie auf der Seite „Volumes“ die Volumes aus, die Sie exportieren möchten, z. B. C:\ und D:\, und klicken Sie dann auf **Weiter**.

9 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

HINWEIS: Sie können den Status und Fortschritt des Exports auf der Registerkarte „Virtual Standby“ oder auf der Registerkarte „Ereignisse“ überwachen.

Durchführen eines kontinuierlichen VirtualBox-Exports (Virtual Standby)

Führen Sie die folgenden Schritte aus, um ein Virtual Standby zu erstellen und einen kontinuierlichen VirtualBox-Export durchzuführen.

So führen Sie einen kontinuierlichen VirtualBox-Export (Virtual Standby) durch

1 Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:

- Klicken Sie auf der Registerkarte „Virtual Standby“ auf **Hinzufügen** klicken, um den Exportassistenten zu starten. Wählen Sie auf der Seite „Geschützte Maschinen“ des Exportassistenten die geschützte Maschine aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.

- Navigieren Sie zu der Maschine, die exportiert werden soll, und klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü „Aktionen“ der betreffenden Maschine auf **Export** > **Virtual Standby**.

2 Wählen Sie auf der Seite „Ziel“ des Exportassistenten im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ **VirtualBox** aus und klicken Sie auf **Weiter**.

3 Wählen Sie auf der Seite „Optionen für virtuelle Maschine“ **Windows-Maschine verwenden** aus.

4 Geben Sie die Parameter für den Zugriff auf die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 80.

Option	Beschreibung
Name der virtuellen Maschine	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein. **HINWEIS:** Standardmäßig wird der Name der Quellmaschine verwendet.
Zielpfad	Geben Sie einen lokalen oder Remote-Zielpfad für die Erstellung der virtuellen Maschine an. **HINWEIS:** Der Zielpfad darf kein Stammverzeichnis sein. Wenn Sie einen Netzwerkfreigabepfad angegeben haben, müssen Sie gültige Anmeldeinformationen (Benutzername und Konto) für ein Konto eingeben, das auf der Zielmaschine registriert ist. Das Konto muss über Lese- und Schreibberechtigungen für die Netzwerkfreigabe verfügen.
Arbeitsspeicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • **Gleiche RAM-Größe verwenden wie Quellmaschine** • **„Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben** Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.

5 Wählen Sie **Benutzerkonto für die exportierte virtuelle Maschine angeben** aus, um ein Benutzerkonto für die virtuelle Maschine anzugeben, und geben Sie die folgenden Informationen ein. Hierbei handelt es sich um ein bestimmtes Benutzerkonto, für das die virtuelle Maschine registriert wird, falls auf der virtuellen Maschine mehrere Benutzerkonten vorhanden sind. Nur der Benutzer, der sich mit diesem Benutzerkonto anmeldet, kann die betreffende virtuelle Maschine im VirtualBox-Manager sehen. Wird kein Konto angegeben, wird die virtuelle Maschine für alle vorhandenen Benutzer auf der Windows-Maschine mit VirtualBox registriert.

- **Benutzername**: Geben Sie den Benutzernamen ein, für den die virtuelle Maschine registriert wird.
- **Kennwort**: Geben Sie das Kennwort für dieses Konto ein.

6 Wählen Sie **Ersten Ad-Hoc-Export durchführen**, um den virtuellen Export sofort und nicht nach dem nächsten geplanten Snapshot durchzuführen.

7 Klicken Sie auf **Weiter**.

8 Wählen Sie auf der Seite „Volumes“ die Volumes aus, die Sie exportieren möchten, z. B. C:\ und D:\, und klicken Sie dann auf **Weiter**.

9 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

HINWEIS: Sie können den Status und Fortschritt des Exports auf der Registerkarte „Virtual Standby“ oder auf der Registerkarte „Ereignisse“ überwachen.

Exportieren von Sicherungsinformationen aus einer Linux-Maschine in eine virtuelle Maschine

Mit AppAssure können Sie Daten einer Linux-Maschine in eine virtuelle VirtualBox-Maschine exportieren. Ein Export umfasst alle Sicherungsdaten eines Wiederherstellungspunkts sowie die für den Schutzzeitplan der Maschine definierten Parameter.

HINWEIS: Es wird VirtualBox, Version 4.2.18 oder höher unterstützt. Der Export für Linux setzt eine SSH-Verbindung vom Core zur Linux-Maschine voraus, wenn die Linux-Maschine als VirtualBox-Host verwendet wird.

Durchführen eines einmaligen VirtualBox-Exports

Führen Sie die folgenden Schritte aus, um einen einmaligen VirtualBox-Export durchzuführen.

So führen Sie einen einmaligen VirtualBox-Export durch

1. Navigieren Sie in der AppAssure Core Console zu der Linux-Maschine, die Sie exportieren möchten.
2. Klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü „Aktionen“ für die jeweilige Maschine auf **Export** und wählen Sie dann **Einmalig** aus.

   Im Exportassistenten wird die Seite „Geschützte Maschinen“ angezeigt.
3. Wählen Sie eine Maschine für den Export aus und klicken Sie dann auf **Weiter**.
4. Wählen Sie auf der Seite „Wiederherstellungspunkte“ den Wiederherstellungspunkt aus, den Sie exportieren möchten, und klicken Sie dann auf **Weiter**.
5. Wählen Sie auf der Seite „Ziel“ des Exportassistenten im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ **VirtualBox** aus und klicken Sie auf **Weiter**.
6. Wählen Sie auf der Seite „Optionen für virtuelle Maschine“ **Remote-Linux-Maschine** aus, falls eine SSH-Verbindung verwendet wird.
7. Geben Sie die Informationen für die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 81.

Option	Beschreibung
VirtualBox-Hostname	Geben Sie eine IP-Adresse oder einen Hostnamen für den VirtualBox-Server ein. Dabei handelt es sich um die IP-Adresse oder den Hostnamen des Remote-VirtualBox-Servers.
Port	Geben Sie eine Portnummer für die Maschine ein. Diese Nummer gibt den Port an, über den der Core mit der Maschine kommuniziert.
Name der virtuellen Maschine	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein. **HINWEIS:** Standardmäßig wird der Name der Quellmaschine verwendet.
Zielpfad	Geben Sie Zielpfad für die Erstellung der virtuellen Maschine an. **HINWEIS:** Es wird empfohlen, einen Stammordner im Stammverzeichnis zu erstellen, sodass die virtuelle Maschine im Stammverzeichnis ausgeführt wird. Wenn Sie nicht das Stammverzeichnis verwenden, müssen Sie den Zielordner auf der Zielmaschine manuell erstellen, bevor Sie den Export einrichten. Darüber hinaus müssen Sie die virtuelle Maschine nach dem Export manuell laden.
Benutzername	Benutzername des Kontos auf der Zielmaschine, z. B. „root“.

Tabelle 81.

Option	Beschreibung
Kennwort	Kennwort für das Benutzerkonto auf der Zielmaschine.
Arbeitsspeicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • **Gleiche RAM-Größe verwenden wie Quellmaschine** • **„Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben** Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.

8 Wählen Sie auf der Seite „Volumes“ die Volumes mit den Daten aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.

9 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

ⓘ **HINWEIS:** Sie können den Status und Fortschritt des Exports auf der Registerkarte „Virtual Standby“ oder auf der Registerkarte „Ereignisse“ überwachen.

Durchführen eines kontinuierlichen VirtualBox-Exports (Virtual Standby)

Führen Sie die folgenden Schritte aus, um ein Virtual Standby zu erstellen und einen kontinuierlichen VirtualBox-Export durchzuführen.

So führen Sie einen kontinuierlichen VirtualBox-Export (Virtual Standby) durch

1 Führen Sie in der AppAssure Core Console eine der folgenden Aktionen aus:

- Klicken Sie auf der Registerkarte „Virtual Standby“ auf **Hinzufügen** klicken, um den Exportassistenten zu starten. Wählen Sie auf der Seite „Geschützte Maschinen“ des Exportassistenten die geschützte Maschine aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.
- Navigieren Sie zu der Maschine, die exportiert werden soll, und klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü „Aktionen“ der betreffenden Maschine auf **Export** > **Virtual Standby**.

2 Wählen Sie auf der Seite „Ziel“ des Exportassistenten im Dropdown-Menü „Wiederherstellung auf eine virtuelle Maschine“ **VirtualBox** aus.

3 Wählen Sie auf der Seite „Optionen für virtuelle Maschine“ **Remote-Linux-Maschine** aus.

4 Geben Sie die Informationen für die virtuelle Maschine ein (siehe Beschreibung in der folgenden Tabelle).

Tabelle 82.

Option	Beschreibung
VirtualBox-Hostname	Geben Sie eine IP-Adresse oder einen Hostnamen für den VirtualBox-Server ein. Dabei handelt es sich um die IP-Adresse oder den Hostnamen des Remote-VirtualBox-Servers.
Port	Geben Sie eine Portnummer für die Maschine ein. Diese Nummer gibt den Port an, über den der Core mit der Maschine kommuniziert.
Name der virtuellen Maschine	Geben Sie den Namen für die zu erstellende virtuelle Maschine ein. **HINWEIS:** Standardmäßig wird der Name der Quellmaschine verwendet.

Tabelle 82.

Option	Beschreibung
Zielpfad	Geben Sie Zielpfad für die Erstellung der virtuellen Maschine an. **HINWEIS:** Es wird empfohlen, einen Stammordner im Stammverzeichnis zu erstellen, sodass die virtuelle Maschine im Stammverzeichnis ausgeführt wird. Wenn Sie nicht das Stammverzeichnis verwenden, müssen Sie den Zielordner auf der Zielmaschine manuell erstellen, bevor Sie den Export einrichten. Darüber hinaus müssen Sie die virtuelle Maschine nach dem Export manuell laden.
Benutzername	Benutzername des Kontos auf der Zielmaschine, z. B. „root“.
Kennwort	Kennwort für das Benutzerkonto auf der Zielmaschine.
Arbeitsspeicher	Geben Sie den Arbeitsspeicher für die virtuelle Maschine an. Sie haben folgende Auswahlmöglichkeiten: • **Gleiche RAM-Größe verwenden wie Quellmaschine** • **„Bestimmte RAM-Größe verwenden“ auswählen und Größe in MB eingeben** Die minimale Größe beträgt 1024 MB, die von der Anwendung maximal nutzbare Größe beträgt 65536 MB. Die maximal nutzbare Größe wird durch die Größe des verfügbaren Arbeitsspeichers in der Hostmaschine beschränkt.

5 Wählen Sie **Ersten Ad-Hoc-Export durchführen**, um den virtuellen Export sofort und nicht nach dem nächsten geplanten Snapshot durchzuführen.

6 Klicken Sie auf **Weiter**.

7 Wählen Sie auf der Seite „Volumes“ die Volumes mit den Daten aus, die Sie exportieren möchten, und klicken Sie dann auf **Weiter**.

8 Klicken Sie auf der Seite „Zusammenfassung“ auf **Fertigstellen**, um den Assistenten zu schließen und den Export zu starten.

HINWEIS: Sie können den Status und Fortschritt des Exports auf der Registerkarte „Virtual Standby“ oder auf der Registerkarte „Ereignisse“ überwachen.

Grundlegende Informationen zur BMR-Wiederherstellung

Server erledigen die Aufgaben, für die sie vorgesehen sind, nur, wenn sie einwandfrei und fehlerfrei funktionieren. Wenn ein Server durch eine Notfallsituation oder durch eine Störung ausfällt, müssen unverzüglich entsprechende Maßnahme durchgeführt werden, um die volle Funktionsfähigkeit der Maschine wiederherzustellen.

AppAssure bietet die Möglichkeit, eine BMR-Wiederherstellung (Bare Metal Restore) für Windows- oder Linux-Maschinen durchzuführen. Bei einer BMR-Wiederherstellung wird die vollständige Softwarekonfiguration eines bestimmten Systems wiederhergestellt. Der Begriff „Bare Metal“ soll verdeutlichen, dass bei der Wiederherstellung nicht nur die Daten des Servers wiederhergestellt werden, sondern auch Festplattenlaufwerke neu formatiert sowie Betriebssystem und alle Softwareanwendungen neu installiert werden. Um eine BMR-Wiederherstellung durchzuführen, geben Sie einen Wiederherstellungspunkt einer geschützten Maschine an und führen Sie ein Rollback (Durchführung einer Wiederherstellung) auf die angegebene physische oder virtuelle Maschine durch. Bei der Durchführung einer Wiederherstellung auf ein System-Volume handelt es sich um eine BMR-Wiederherstellung. Wenn bei der Durchführung einer Wiederherstellung eine Start-CD erforderlich ist, handelt es sich ebenfalls um eine BMR-Wiederherstellung. Zu anderen Situationen, in denen Sie u. U. eine BMR-Wiederherstellung durchführen möchten, zählen Hardware-Upgrades oder der Austausch eines Servers. In beiden Fällen wird eine Wiederherstellung aus einem Wiederherstellungspunkt auf die aktualisierte oder ersetzte Hardware durchgeführt.

AppAssure ermöglicht Schutz und Wiederherstellung der Betriebssysteme Windows 8, 8.1 und Windows Server 2012, 2012 R2, die von FAT32-EFI-Partitionen gestartet werden, sowie von ReFS-Volumes (Resilient File System).

HINWEIS: Eine BMR-Wiederherstellung (Bare Metal Restore) der Festplattenkonfiguration für Speicherplätze (eine Funktion von Windows 8.1) wird in diesem Release ebenfalls nicht unterstützt.

Zurzeit werden lediglich vollständige Wiederherstellung und BMR-Wiederherstellung unterstützt, da es bei ReFS Treibereinschränkungen gibt, sodass Wiederherstellung, VM-Export usw. im Benutzermodus implementiert sind. Wenn ein Core mindestens ein Agent-Volume schützt, das das Dateisystem ReFS enthält, muss die Installation auf einer Maschine mit Windows 8, Windows 8.1, Windows Server 2012 oder Windows Server 2012 R2 erfolgen, da diese Betriebssysteme ReFS nativ unterstützen. Andernfalls ist die Funktionalität begrenzt und Vorgänge, bei denen beispielsweise ein Volume-Image bereitgestellt werden muss, funktionieren nicht. In diesem Fall werden in der AppAssure Core Console entsprechende Fehlermeldungen angezeigt.

Nur unterstützte Linux-Betriebssysteme können geschützt und wiederhergestellt werden. Dazu gehören Ubuntu, Red Hat Enterprise Linux, CentOS und SUSE Linux Enterprise Server (SLES). Details finden Sie im *Dell AppAssure Bereitstellungshandbuch*.

eine BMR-Wiederherstellung kann für physische oder virtuelle Maschinen durchgeführt werden. Ein weiterer Vorteil besteht darin, dass Sie mit AppAssure eine BMR-Wiederherstellung unabhängig davon durchführen können, ob die Hardware *vergleichbar* oder *unterschiedlich* ist. Bei der Durchführung einer BMR-Wiederherstellung in AppAssure wird das Betriebssystem von einer bestimmten Plattform getrennt, sodass das System portabel wird.

Beispiele für eine BMR-Wiederherstellung für vergleichbare Hardware sind u. a. der Austausch der Festplatte eines vorhandenen Systems oder der Ersatz eines ausgefallenen Servers durch eine identische Maschine.

Beispiele für eine BMR-Wiederherstellung für andere Hardware sind u. a. die Wiederherstellung eines ausgefallenen Systems durch einen Server eines anderen Herstellers oder mit einer anderen Konfiguration. Dieser Vorgang umfasst das Erstellen eines Start-CD-Image, das Brennen des Image auf einen Datenträger, das Starten des Zielservers vom Start-Image, das Herstellen einer Verbindung zur Recovery Console-Instanz, das Zuordnen von Volumes, die Initiierung der Wiederherstellung und anschließend die Überwachung des Vorgangs. Nachdem die BMR-Wiederherstellung durchgeführt wurde, können Sie das Betriebssystem und die Softwareanwendungen auf den wiederhergestellten Server laden sowie die erforderlichen Einstellungen für die jeweilige Konfiguration vornehmen.

Die BMR-Wiederherstellung wird nicht nur in Notfallwiederherstellungsszenarien verwendet, sondern auch bei der Migration von Daten beim Upgrade oder Austausch von Servern.

Obwohl eine BMR-Wiederherstellung für virtuelle Maschinen unterstützt wird, muss darauf hingewiesen werden, dass die Durchführung eines virtuellen Exports für eine VM einfacher ist als eine BMR-Wiederherstellung auf einer physischen Maschine. Weitere Informationen zum Durchführen eines VM-Exports für virtuelle Maschinen finden Sie in der Beschreibung für die jeweilige VM.

- Weitere Informationen zum Durchführen eines VM-Exports mit ESXi finden Sie unter Exportieren von Windows-Daten mit ESXi-Export.
- Weitere Informationen zum Durchführen eines VM-Exports mit VMware Workstation finden Sie unter Exportieren von Windows-Daten mit VMware Workstation-Export.
- Weitere Informationen zum Durchführen eines VM-Exports mit Hyper-V finden Sie unter Exportieren von Windows-Daten mit Hyper-V-Export.
- Weitere Informationen zum Durchführen eines VM-Exports mit VirtualBox finden Sie unter Exportieren von Windows-Daten nach VirtualBox.
- Weitere Informationen zum Durchführen eines VM-Exports für eine geschützte Linux-Maschine finden Sie unter Exportieren von Sicherungsinformationen aus einer Linux-Maschine in eine virtuelle Maschine.

Informationen zum Durchführen einer BMR-Wiederherstellung auf einer Windows-Maschine finden Sie in der betreffenden Windows-Anleitung. Dort werden auch die Voraussetzungen beschrieben. Weitere Informationen finden Sie unter Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen.

Sie können auch mit dem Assistenten zum Wiederherstellen einer Maschine eine BMR-Wiederherstellung durchführen. Führen Sie dazu zunächst die in Wiederherstellen von Volumes aus einem Wiederherstellungspunkt

beschriebenen Schritte durch und wechseln Sie an der dort genannten Stelle zu Verwalten eines Windows-Start-Image und Starten einer BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine.

Informationen zum Durchführen einer BMR-Wiederherstellung auf einer Linux-Maschine finden Sie in der betreffenden Linux-Anleitung. Dort werden auch die Voraussetzungen beschrieben. Neben einer BMR-Wiederherstellung mit dem Befehlszeilenprogramm „aamount“ können Sie eine BMR-Wiederherstellung jetzt auch in der Benutzeroberfläche der Core Console durchführen. In der Anleitung werden beide Verfahren behandelt. Weitere Informationen finden Sie unter Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen.

Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen

Um eine BMR-Wiederherstellung für Windows-Maschinen durchzuführen, müssen Sie die folgenden Aufgaben durchführen.

- **Verwalten eines Windows-Start-Image**. Das ISO-Image der Start-CD wird zum Starten des Ziellaufwerks verwendet. Von dort aus können Sie auf die Universal Recovery Console zugreifen, um Sicherungen auf dem Core zu übertragen. Siehe Verwalten eines Windows-Start-Image.
    - Wenn zum Starten der Zielmaschine ein physischer Datenträger erforderlich ist, müssen Sie weiterhin **das ISO-Image für die Start-CD auf ein Medium übertragen**. Siehe Übertragen des ISO-Image der Start-CD auf Datenträger.
    - In allen Fällen müssen Sie **das Start-Image im Zielserver laden und den Server vom Start-Image starten**. Siehe Laden der Start-CD und Starten der Zielmaschine.
- **Starten einer BMR-Wiederherstellung für Windows**. Nachdem die Zielmaschine von der Start-CD gestartet wurde, können Sie die BMR-Wiederherstellung starten. Siehe Starten einer BMR-Wiederherstellung für Linux.
    - Sie müssen **eine Wiederherstellung aus einem Wiederherstellungspunkt im Core einleiten**. Siehe Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung.
    - Anschließend müssen Sie die **Volumes zuordnen**. Siehe Zuordnen von Volumes für eine BMR-Wiederherstellung.
    - Wenn bei einer Wiederherstellung auf einer unterschiedlichen Hardware die erforderlichen Speicher- und Netzwerktreiber nicht auf der Start-CD vorhanden sind, müssen Sie die Treiber u. U. von einem Wechselmedium laden. Weitere Informationen finden Sie unter Laden von Treibern mit der Universal Recovery Console.
    - Wenn bei einer Wiederherstellung auf einer unterschiedlichen Hardware alle erforderlichen Treiber auf der Start-CD vorhanden sind, müssen Sie die **Treiber für Hardwaregeräte injizieren**, die in der vorherigen Konfiguration nicht vorhanden waren, aber im Ersatzsystem für den Server enthalten sind. Weitere Informationen finden Sie unter Injizieren von Treibern auf dem Zielserver.
- **BMR-Wiederherstellung mit dem Assistenten zum Wiederherstellen einer Maschine durchführen**. Die Schritte zum Verwalten eines Windows-Start-Image und zum Starten der BMR-Wiederherstellung (mit allen untergeordneten Aufgaben) können mit dem Assistenten zum Wiederherstellen einer Maschine durchgeführt werden. Informationen zum Starten des Assistenten finden Sie in den Schritten 1 bis 5 von Wiederherstellen von Volumes aus einem Wiederherstellungspunkt. Die weiteren Informationen finden Sie unter Verwalten eines Windows-Start-Image und Starten einer BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine.
- **Überprüfen einer BMR-Wiederherstellung**. Nachdem die BMR-Wiederherstellung (Bare Metal Restore) gestartet wurde, können Sie den Fortschritt überprüfen und überwachen. Siehe Überprüfen einer BMR-Wiederherstellung.
    - Sie können den **Fortschritt der Wiederherstellung überwachen**. Siehe Anzeigen des Fortschritts der Wiederherstellung.

- Danach können Sie **den wiederhergestellten Server starten**. Siehe Starten eines wiederhergestellten Zielservers.
- **Beheben von Fehlern beim BMR**. Siehe Beheben von Universal Recovery Console-Verbindungsproblemen und Reparieren von Startproblemen.

Voraussetzungen für eine BMR-Wiederherstellung für Windows-Maschinen

Damit Sie eine BMR-Wiederherstellung (Bare Metal Restore) für eine Windows-Maschine durchführen können, müssen die folgenden Bedingungen und Kriterien erfüllt sein:

- **Vorhandensein von Sicherungen der Maschine, die wiederhergestellt werden soll.** Es muss ein funktionierender AppAssure Core mit Wiederherstellungspunkten des geschützten Servers vorhanden sein, der wiederhergestellt werden soll.
- **Hardware für die Wiederherstellung (neu oder alt, vergleichbar oder unterschiedlich).** Die Zielmaschine muss die Installationsanforderungen für einen Agenten erfüllen. Entsprechende Details finden Sie im *Dell AppAssure Bereitstellungshandbuch*.
- **Image-Datenträger und -Software.** Sie müssen über eine leere CD oder DVD sowie über eine Software zum Brennen von Datenträgern oder eine Software zum Erstellen eines ISO-Image verfügen. Wenn Sie Maschinen remote mit einer virtuellen Vernetzungssoftware wie UltraVNC verwalten, benötigen Sie einen VNC-Viewer.
- **Kompatible Speichertreiber und Netzwerkadaptertreiber.** Bei der Wiederherstellung auf unterschiedlicher Hardware müssen ggf. Speichertreiber und Netzwerkadaptertreiber (z. B. RAID, AHCI) für die Zielmaschine sowie Chipsatztreiber für das Zielbetriebssystem vorhanden sein, die kompatibel mit Windows 7 PE (32-Bit) sind.
- **Speicherplatz und Partitionen je nach Bedarf.** Auf der Zielfestplatte muss genügend Speicherplatz zum Erstellen der Zielpartitionen auf der Zielmaschine für die Quell-Volumes vorhanden sein. Jede Zielpartition muss mindestens so groß sein wie die ursprüngliche Quellpartition.
- **Kompatible Partitionen.** Windows 8-, Windows 8.1-, Windows Server 2012- und Windows Server 2012 R2-Betriebssysteme, die von FAT32-EFI-Partitionen gestartet werden, sowie ReFS-Volumes (Resilient File System) können geschützt und wiederhergestellt werden. UEFI-Partitionen werden als einfache FAT32-Volumes behandelt. Inkrementelle Übertragungen werden vollständig unterstützt und geschützt. AppAssure unterstützt UEFI-Systems für BMR, einschließlich der automatischen Partitionierung von GPT-Datenträgern.

Verwalten eines Windows-Start-Image

Für eine BMR-Wiederherstellung (Bare Metal Restore) für Windows ist ein Start-Image (Start-CD genannt) erforderlich, das Sie durch Festlegen der entsprechenden Parameter in der AppAssure Core Console erstellen können. Dieses Image wird an die jeweiligen Anforderungen angepasst. Mit dem Image wird die Windows-Zielmaschine gestartet. Abhängig von den jeweiligen Eigenschaften der Umgebung müssen Sie dieses Image u. U. auf ein physisches Medium übertragen (z. B. CD oder DVD). Anschließend müssen Sie das Start-Image virtuell oder physisch laden und den Windows-Server mit dem Start-Image starten.

Dies ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen.

Um ein Windows-Start-Image zu erhalten, können Sie die folgenden Aufgaben durchführen:

- Erstellen eines ISO-Image für eine Start-CD für Windows
- Festlegen der Parameter für das ISO-Image der Start-CD
- Übertragen des ISO-Image der Start-CD auf Datenträger
- Laden der Start-CD und Starten der Zielmaschine

HINWEIS: In diesem Prozess wird beschrieben, wie ein Start-CD-Image im Dialogfeld „Start-CD erstellen“ verwaltet wird. Sie können diese Schritte auch im Assistenten zum Wiederherstellen einer Maschine durchführen (ab der Start-CD-Seite des Assistenten). Diese Seite wird angezeigt, wenn Sie auf der Seite „Ziel“ des Assistenten **Wiederherstellung auf einer beliebigen Zielmaschine mit einer Start-CD** auswählen.

Schrittweise Anweisungen zum Verwalten eines Windows-Start-Image im Assistenten zum Wiederherstellen einer Maschine im Rahmen einer BMR-Wiederherstellung finden Sie unter Verwalten eines Windows-Start-Image und Starten einer BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine.

Erstellen eines ISO-Image für eine Start-CD für Windows

Bei der Durchführung einer BMR-Wiederherstellung (Bare Metal Restore) für eine Windows-Maschine muss als Erstes die Start-CD-Datei in der AppAssure Core Console erstellt werden. Dabei handelt es sich um ein startfähiges ISO-Image, das die AppAssure Universal Recovery Console (URC) enthält, eine Umgebung, mit der das Systemlaufwerk oder ein ganzer Server direkt vom AppAssure Core aus wiederhergestellt werden kann.

Das erstellte ISO-Image für die Start-CD wird an die Maschine angepasst, die wiederhergestellt wird, und muss daher die richtigen Netzwerk- und Massenspeichertreiber enthalten. Wenn vorhersehbar ist, dass die Wiederherstellung auf einer anderen Hardware als der Maschine erfolgt, von der der Wiederherstellungspunkt stammt, müssen Sie Speichercontroller- und andere Treiber in die Start-CD aufnehmen. Informationen zum Injizieren dieser Treiber in die Start-CD finden Sie unter Injizieren von Treibern in eine Start-CD.

HINWEIS: Die ISO (International Organization for Standardization) ist eine internationale Organisation von Vertretern aus verschiedenen nationalen Organisationen, die Normen für Dateisysteme festlegt. ISO 9660 ist eine Norm für Dateisysteme, die für optische Datenträger zum Austausch von Daten verwendet wird und mehrere Betriebssysteme unterstützt, z. B. Windows. Ein ISO-Image ist die Archivdatei oder das Datenträger-Image, das die Daten der einzelnen Sektoren sowie das Dateisystem des Datenträgers enthält.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten eines Windows-Start-Image.

So erstellen Sie ein ISO-Image für die Start-CD

1. Wählen Sie in der AppAssure Core Console, in der der wiederherzustellende Server geschützt ist, den Core und dann die Registerkarte „Extras“ aus.
2. Klicken Sie auf **Start-CDs**.
3. Wählen Sie **Aktionen** aus und klicken Sie dann auf **Start-CD erstellen**.

   Das Dialogfeld „Start-CD erstellen“ wird angezeigt. Gehen Sie folgendermaßen vor, um das Dialogfeld auszufüllen.

Festlegen der Parameter für das ISO-Image der Start-CD

Im Dialogfeld „Start-CD erstellen“ müssen ggf. mehrere Parameter angegeben werden. Führen Sie abhängig von der jeweiligen Situation die folgenden Aufgaben durch, um die Eigenschaften des ISO-Image der Start-CD für eine BMR-Wiederherstellung festzulegen.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Erstellen eines ISO-Image für eine Start-CD für Windows.

Benennen der Start-CD-Datei und Festlegen des Pfads

Führen Sie den folgenden Schritt aus, um den Namen der Start-CD-Datei und den Pfad festzulegen, in dem das ISO-Image gespeichert wird.

Diese Aufgabe ist ein Schritt im Prozess Festlegen der Parameter für das ISO-Image der Start-CD. Dieser ist Bestandteil des Prozesses zum Erstellen eines ISO-Image für eine Start-CD für Windows.

So benennen Sie die Start-CD-Datei und legen Sie den Pfad fest

- Geben Sie im Dialogfeld „Start-CD erstellen“ unter „Ausgabeoptionen“ im Textfeld „Ausgabepfad“ den Pfad ein, in dem das ISO-Image der Start-CD auf dem Core-Server gespeichert werden soll.

  Wenn auf dem freigegebenen Laufwerk, auf der das Image gespeichert werden soll, nicht genügend Speicherplatz vorhanden ist, können Sie den Pfad nach Bedarf anpassen, z. B. D:\Dateiname.iso.

  HINWEIS: Die Dateierweiterung muss .iso sein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche, umgekehrte Schrägstriche (nur als Pfadtrennzeichen) und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

Erstellen von Verbindungen

Führen Sie die folgenden Schritte aus, um die Verbindungen zu erstellen.

Diese Aufgabe ist ein Schritt im Prozess Festlegen der Parameter für das ISO-Image der Start-CD. Dieser ist Bestandteil des Prozesses zum Erstellen eines ISO-Image für eine Start-CD für Windows.

So erstellen Sie Verbindungen

1 Führen Sie unter „Verbindungsoptionen“ eine der folgenden Aktionen aus:

   - Wählen Sie **IP-Adresse automatisch beziehen** aus, um die IP-Adresse dynamisch von DHCP (Dynamic Host Configuration Protocol) zu beziehen.
   - Wählen Sie ggf. **Folgende IP-Adresse verwenden** aus, um eine statische IP-Adresse für die Wiederherstellungskonsole anzugeben, und geben Sie IP-Adresse, Subnetzmaske, Standardgateway und DNS-Server in die entsprechenden Felder ein. Sie müssen alle vier Felder ausfüllen.

2 Wählen Sie unter „UltraVNC-Optionen“ ggf. **UltraVNC hinzufügen** aus und geben Sie dann ein UltraVNC-Kennwort und einen UltraVNC-Port an.

   Die UltraVNC-Einstellungen bieten die Möglichkeit, die Wiederherstellungskonsole remote zu verwalten, während sie verwendet wird.

   HINWEIS: Dieser Schritt ist optional. Wenn ein Remote-Zugriff auf die Wiederherstellungskonsole erforderlich ist, müssen Sie UltraVNC konfigurieren und verwenden. Sie können sich nicht über Microsoft-Terminaldienste anmelden, wenn Sie die Start-CD verwenden.

Angeben einer Wiederherstellungsumgebung

Das Start-CD-Image muss so erstellt werden, dass die Start-CD (physisch oder virtuell) auf der Hardware bereitgestellt werden kann, auf der die Wiederherstellung erfolgt. Sie müssen die am besten geeignete Architektur für die betreffende Maschine angeben.

Diese Aufgabe ist ein Schritt im Prozess Festlegen der Parameter für das ISO-Image der Start-CD. Dieser ist Bestandteil des Prozesses zum Erstellen eines ISO-Image für eine Start-CD für Windows.

Führen Sie den folgenden Schritt aus, um eine Wiederherstellungsumgebung anzugeben.

- Wählen Sie unter „Wiederherstellungsumgebung“ eine der Umgebungsoptionen aus (siehe Beschreibung in der folgenden Tabelle).

Tabelle 83.

Option	Beschreibung
Windows-Betriebssystem (64-Bit)	Für die Wiederherstellung auf eine Windows-Maschine mit einer 64-Bit-Architektur (einschließlich Maschinen mit einem UEFI-BIOS)
Windows-Betriebssystem (32-Bit)	Für die Wiederherstellung auf eine Maschine mit einer 32-Bit-Architektur (x86)

Injizieren von Treibern in eine Start-CD

Im Start-CD-Image müssen Speichertreiber vorhanden sein, damit die Laufwerke des Servers erkannt werden, sowie Netzwerkadaptertreiber, damit eine Kommunikation mit dem AppAssure Core über das Netzwerk möglich ist.

Beim Erstellen einer Start-CD für Windows werden automatisch Windows 7 PE 32-Bit-Speichercontroller- und -Netzwerkadaptertreiber hinzugefügt. Dadurch werden die Anforderungen neuerer Dell-Systeme erfüllt. Bei Systemen anderer Hersteller oder älteren Dell-Systemen müssen Sie beim Erstellen der Start-CD u. U. Speichercontroller- oder Netzwerkadaptertreiber hinzufügen. Wenn Sie feststellen, dass die erstellte Start-CD nicht die erforderlichen Treiber für die Wiederherstellung enthält, können Sie die Treiber auch mit der URC auf die Zielmaschine laden. Weitere Informationen finden Sie unter Laden von Treibern mit der Universal Recovery Console.

Beim Erstellen der Start-CD wird die Treiberinjektion verwendet, um die Kommunikation zwischen Recovery Console, Netzwerkadapter und Speicher auf dem Zielserver zu ermöglichen.

Die aus dem Wiederherstellungspunkt wiederhergestellten Daten enthalten die Treiber der zuvor verwendeten Hardware. Bei der Durchführung einer BMR-Wiederherstellung (Bare Metal Restore) auf eine unterschiedliche Hardware müssen Sie mit der URC auch Speichercontrollertreiber in das wiederhergestellte Betriebssystem injizieren, nachdem die Daten auf dem Laufwerk wiederhergestellt wurden, damit das wiederhergestellte Betriebssystem mit der neuen Hardware gestartet werden kann. Nachdem das Betriebssystem nach der Wiederherstellung neu gestartet wurde, können Sie alle weiteren Treiber herunterladen und installieren, die vom Betriebssystem für die Interaktion mit der neuen Hardware benötigt werden.

Weitere Informationen finden Sie unter Injizieren von Treibern auf dem Zielserver.

Diese Aufgabe ist ein Schritt im Prozess Festlegen der Parameter für das ISO-Image der Start-CD. Dieser ist Bestandteil des Prozesses zum Erstellen eines ISO-Image für eine Start-CD für Windows.

Führen Sie die folgenden Schritte aus, um Speichercontroller- und Netzwerkadaptertreiber in eine Start-CD zu injizieren.

So injizieren Sie Treiber in eine Start-CD

1. Laden Sie die Treiber von der Website des Serverherstellers herunter und entpacken Sie sie.
2. Komprimieren Sie jeden Treiber mit einem entsprechenden Programm (z. B. WinZip) in eine .zip-Datei.
3. Klicken Sie im Dialogfeld „Start-CD erstellen“ im Bereich „Treiber“ auf **Treiber hinzufügen**.
4. Navigieren Sie im Dateisystem zur komprimierten Treiberdatei, wählen Sie die Datei aus, und klicken Sie dann auf **Öffnen**.

   Die injizierten Treiber werden im Fensterbereich „Treiber“ hervorgehoben angezeigt.
5. Wiederholen Sie Schritt 3 und Schritt 4 je nach Bedarf, bis alle Treiber injiziert wurden.

Erstellen des ISO-Image für die Start-CD

Diese Aufgabe ist ein Schritt im Prozess Festlegen der Parameter für das ISO-Image der Start-CD. Dieser ist Bestandteil des Prozesses zum Erstellen eines ISO-Image für eine Start-CD für Windows.

Führen Sie den folgenden Schritt aus, um das ISO-Image für die Start-CD zu erstellen.

So erstellen Sie ein ISO-Image für die Start-CD

- Klicken Sie in der Anzeige „Start-CD erstellen“ auf **Start-CD erstellen**, nachdem Name und Pfad der Start-CD-Datei festgelegt, eine Verbindung erstellt und ggf. die Treiber injiziert wurden.

  Daraufhin wird das ISO-Image erstellt und mit dem angegebenen Dateinamen gespeichert.

Anzeigen des Fortschritts der ISO-Image-Erstellung

Diese Aufgabe ist ein Schritt im Prozess Festlegen der Parameter für das ISO-Image der Start-CD. Dieser ist Bestandteil des Prozesses zum Erstellen eines ISO-Image für eine Start-CD für Windows.

Führen Sie den folgenden Schritt aus, um den Fortschritt der Erstellung des ISO-Image anzuzeigen.

So zeigen Sie den Fortschritt der Erstellung des ISO-Image an

- Wählen Sie die Registerkarte „Ereignisse“ aus. Unter „Aufgaben“ können Sie den Fortschritt der Erstellung des ISO-Image überwachen. Weitere Informationen zur Überwachung von AppAssure-Ereignissen finden Sie unter Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen.

  Nachdem das ISO-Image erstellt wurde, wird es auf der Seite „Start-CD“ angezeigt, die im Menü „Extras“ geöffnet werden kann.

Zugreifen auf das ISO-Image

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten eines Windows-Start-Image.

Führen Sie den folgenden Schritt aus, um auf das ISO-Image zuzugreifen.

So greifen Sie auf das ISO-Image zu

- Um auf das ISO-Image zuzugreifen, navigieren Sie zum angegebenen Ausgabepfad. Sie können auch auf den Link klicken, um das Image in einen Speicherort herunterzuladen, von dem aus Sie es auf das neue System laden können, z. B. ein Netzlaufwerk.

Übertragen des ISO-Image der Start-CD auf Datenträger

Wenn Sie die Start-CD-Datei erstellen, wird die Datei im angegebenen Pfad als ISO-Image gespeichert. Sie müssen dieses Image als Laufwerk auf dem Server bereitstellen können, auf dem eine BMR-Wiederherstellung durchgeführt wird.

Sie können das ISO-Image der Start-CD auf CD- oder DVD-Datenträger brennen, die zum Starten des Systems verwendet werden können.

Beim Start der Maschine mit der Start-CD wird automatisch die Universal Recovery Console gestartet.

Bei einer BMR-Wiederherstellung auf einer virtuellen Maschine ist dieser Schritt nicht erforderlich. Laden Sie das ISO-Image einfach in ein Laufwerk und bearbeiten Sie die Einstellungen der VM so, dass sie von diesem Laufwerk aus gestartet wird.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten eines Windows-Start-Image.

Laden der Start-CD und Starten der Zielmaschine

Nachdem das Start-CD-Image erstellt wurde, müssen Sie den Zielserver mit der neu erstellten Start-CD starten.

HINWEIS: Falls Sie die Start-CD mit DHCP erstellt haben, müssen Sie IP-Adresse und Kennwort erfassen.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten eines Windows-Start-Image.

So laden Sie eine Start-CD und starten Sie die Zielmaschine

1. Navigieren Sie zum neuen Server und laden Sie das Start-CD-Image vom jeweiligen Speicherort. Geben Sie an, dass der Server vom Start-CD-Image gestartet wird.
2. Starten Sie die Maschine. Dadurch werden folgenden Komponenten geladen:
   - Windows 7 PE
   - AppAssure Agent-Software

   Die AppAssure Universal Recovery Console wird gestartet und zeigt IP-Adresse sowie Authentifizierungskennwort für die Maschine an.

   HINWEIS: Bei jedem Start der Maschine mit der Start-CD wird ein neues temporäres Kennwort generiert. Notieren Sie sich die im Bereich „Einstellungen für Netzwerkadapter“ angezeigte IP-Adresse und das im Bereich „Authentifizierung“ angezeigte Authentifizierungskennwort. Sie benötigen diese Informationen später bei der Datenwiederherstellung, um sich wieder bei der Konsole anzumelden.
3. Wählen Sie die IP-Adresse aus, wenn Sie diese ändern möchten, und klicken Sie auf **Ändern**.

   HINWEIS: Wenn Sie eine IP-Adresse im Dialogfeld „Start-CD erstellen“ angegeben haben, wird diese Adresse von der Universal Recovery Console verwendet und in der Anzeige „Einstellungen für Netzwerkadapter“ angezeigt.

Nachdem die Maschine mit der Start-CD gestartet wurde, kann vom Core aus eine Verbindung hergestellt und die BMR-Wiederherstellung gestartet werden.

Verwalten eines Windows-Start-Image und Starten einer BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine

Bei der Wiederherstellung von Volumes aus einem Wiederherstellungspunkt mit einer Start-CD oder der Wiederherstellung eines System-Volumes handelt es sich um eine BMR-Wiederherstellung (Bare Metal Restore). Lesen Sie vor einer BMR-Wiederherstellung Voraussetzungen für eine BMR-Wiederherstellung für Windows-Maschinen bzw. Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen durch. Informationen zur BMR-Wiederherstellung auf einer Windows-Maschine in der Core Console finden Sie unter Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen.

Wählen Sie bei einer BMR-Wiederherstellung über den Assistenten zum Wiederherstellen einer Maschine auf der Seite „Ziel“ des Assistenten die Option **Wiederherstellung auf einer beliebigen Zielmaschine mit einer Start-CD** aus und führen Sie anschließend die nachstehend beschriebenen Schritte durch. Die Verwaltung eines Windows-Start-Image über den Assistenten umfasst folgende Schritte: Einleiten der Start-CD-Erstellung, Festlegen des Pfads für das Image auf der Core-Maschine, Auswählen einer geeigneten Wiederherstellungsumgebung für die Hardware, auf der die Wiederherstellung erfolgen soll, Angeben der Verbindungsparameter für den wiederhergestellten Agenten für Netzwerk oder UltraVNC (optional), Injizieren der Treiber für die Hardware, auf der die Wiederherstellung erfolgen soll (optional), und die Übertragung des Start-Image auf physische Medien (optional). Dies umfasst auch das Starten der Maschine von CD, auf der die Daten wiederhergestellt werden sollen, das Herstellen einer Verbindung zur Universal Recovery Console, das Zuordnen von Volumes sowie das Starten einer BMR-Wiederherstellung aus dem ausgewählten Wiederherstellungspunkt auf dem Core.

HINWEIS: Dieser Prozess beschreibt, wie ein Start-CD-Image im Assistenten zum Wiederherstellen einer Maschine bei der Durchführung einer BMR-Wiederherstellung mit dem Assistenten verwaltet wird. Sie können ein Start-Image auch im Dialogfeld „Start-CD erstellen“ verwalten. Informationen zum Verwalten eines Start-CD-Image außerhalb des Assistenten zum Wiederherstellen einer Maschine finden Sie unter Verwalten eines Windows-Start-Image.

So verwalten Sie ein Windows-Start-Image und starten Sie eine BMR-Wiederherstellung im Assistenten zum Wiederherstellen einer Maschine

1 Führen Sie auf der Seite „Start-CD“ die folgenden Aktionen aus:

a Geben Sie im Feld **Ausgabepfad** den Pfad ein, in dem das ISO-Image der Start-CD gespeichert werden soll.

Wenn auf dem freigegebenen Laufwerk, auf der das Image gespeichert werden soll, nicht genügend Speicherplatz vorhanden ist, können Sie den Pfad nach Bedarf anpassen, z. B. D:\Dateiname.iso.

HINWEIS: Die Dateierweiterung muss .iso sein. Verwenden Sie in der Pfadangabe nur alphanumerische Zeichen, Bindestriche, umgekehrte Schrägstriche (nur als Pfadtrennzeichen) und Punkte (nur zum Trennen von Hostnamen und Domänen). Bei den Buchstaben a bis z wird keine Groß-/Kleinschreibung unterschieden. Verwenden Sie keine Leerzeichen. Andere Symbole oder Interpunktionszeichen sind nicht zulässig.

b Wählen Sie unter **Umgebung** die am besten geeignete Architektur für die Hardware aus, auf der die Wiederherstellung erfolgt:

- Wählen Sie für eine Wiederherstellung auf einer Windows-Maschine mit einer 64-Bit-Architektur **Windows 8 64-Bit (erforderlich für Maschinen, die mit einem UEFI BIOS konfiguriert sind)** aus.
- Wählen Sie bei einer Wiederherstellung auf eine Maschine mit einer 32-Bit-Architektur (x86) **Windows 7 32-Bit** aus.

2 Wählen Sie ggf. **Erweiterte Optionen anzeigen** aus, um Netzwerkparameter für den wiederhergestellten Agenten einzurichten oder UltraVNC zu verwenden, und führen Sie eine der folgenden Aktionen aus:

- Wählen Sie **Folgende IP-Adresse verwenden** aus, um eine Netzwerkverbindung zur wiederhergestellten Maschine einzurichten, und geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

Tabelle 84.

Option	Beschreibung
IP-Adresse	Geben Sie eine IP-Adresse oder einen Hostnamen für die wiederhergestellte Maschine ein.
Subnetzmaske	Geben Sie die Subnetzmaske für die wiederhergestellte Maschine ein.
Standardgateway	Geben Sie das Standardgateway für die wiederhergestellte Maschine ein.
DNS-Server	Geben Sie den DNS-Server für die wiederhergestellte Maschine ein.

- Wählen Sie **UltraVNC hinzufügen** aus, um UltraVNC-Informationen festzulegen, und geben Sie die in der folgenden Tabelle beschriebenen Informationen ein.

  Verwenden Sie diese Option, wenn ein Remote-Zugriff auf die Wiederherstellungskonsole erforderlich ist. Sie können sich nicht über Microsoft-Terminaldienste anmelden, wenn Sie die Start-CD verwenden.

Tabelle 85.

Option	Beschreibung
Kennwort	Geben Sie ein Kennwort für die UltraVNC-Verbindung ein.
Port	Geben Sie einen Port für die UltraVNC-Verbindung ein. Die Standardportnummer ist 5900.

3 Wenn Sie die gewünschten Optionen auf der Seite „Start-CD“ festgelegt haben, klicken Sie auf **Weiter**.

4 Führen Sie auf der Seite „Treiberinjektion“ ggf. die folgenden Aktionen durch, um einen Treiber hinzuzufügen:

   a Wählen Sie **Treiberarchiv hinzufügen** aus.

   b Navigieren Sie zur ZIP-Datei mit dem Archiv, wählen Sie die ZIP-Datei aus, und klicken Sie auf **Öffnen**.

   Das Archiv wird geladen und auf der Seite „Treiberinjektion“ angezeigt.

   c Klicken Sie anschließend auf **Weiter**.

5 Auf der Seite „ISO-Image“ wird der Status der Erstellung des ISO-Image für die Start-CD angezeigt. Klicken Sie auf **Weiter**, wenn die Start-CD erfolgreich erstellt wurde.

Die Seite „Verbindung“ wird angezeigt.

6 An dieser Stelle sollten Sie die Agent-Maschine, auf der die Daten wiederhergestellt werden sollen, mit der Start-CD starten.

- Wenn Sie die Agent-Maschine vom ISO-Image der Start-CD starten können, starten Sie die Maschine jetzt.
- Kopieren Sie das ISO-Image andernfalls auf ein physisches Medium (CD oder DVD) und legen Sie den Datenträger in die Agent-Maschine ein. Konfigurieren Sie die Maschine so, dass die Start-CD geladen wird, und führen Sie einen Neustart von der Start-CD durch.

  HINWEIS: Sie müssen u. U. die BIOS-Einstellungen der Agent-Maschine ändern, damit die Start-CD als erstes Volume geladen wird.

  Beim Start von der Start-CD wird auf der Agent-Maschine die URC-Oberfläche (Universal Recovery Console) angezeigt. Diese Umgebung wird verwendet, um das Systemlaufwerk bzw. die ausgewählten Volumes direkt vom AppAssure Core wiederherzustellen. Die IP-Adresse und der Authentifizierungsschlüssel für die Anmeldung werden bei jedem Start mit der Start-CD in der URC geändert.

7 Geben Sie in der Core Console auf der Seite „Verbindung“ die Authentifizierungsinformationen der URC-Instanz der Maschine, die wiederhergestellt werden soll, wie folgt ein:

   a Geben Sie im Textfeld „IP-Adresse“ die IP-Adresse der Maschine ein, die aus einem Wiederherstellungspunkt wiederhergestellt wird.

   b Geben Sie im Textfeld „Authentifizierungsschlüssel“ die Informationen aus der URC ein.

   c Klicken Sie anschließend auf **Weiter**.

Die Seite „Datenträgerzuordnung“ wird angezeigt.

8 Wenn Volumes automatisch zugeordnet werden sollen, gehen Sie wie folgt vor. Wenn Volumes manuell zugeordnet werden sollen, fahren Sie mit Schritt 9 fort.

   a Wählen Sie **Automatische Volume-Zuordnung** aus.

   b Wählen Sie im Bereich „Automatische Volume-Zuordnung“ auf der linken Seite die Volumes aus, die wiederhergestellt werden sollen. Deaktivieren Sie die Option, wenn Sie ein aufgelistetes Volume nicht wiederherstellen möchten.

   HINWEIS: Zum Durchführen der Wiederherstellung muss mindestens ein Volume ausgewählt werden.

c Wählen Sie auf der rechten Seite den Zieldatenträger für die Wiederherstellung aus.

d Klicken Sie auf **Weiter** und gehen Sie zu Schritt Schritt 10.

9 Wenn Volumes manuell zugeordnet werden sollen, gehen Sie wie folgt vor:

a Wählen Sie **Manuelle Volume-Zuordnung** aus.

b Wählen Sie im Bereich „Manuelle Volume-Zuordnung“ in der Dropdown-Liste „Ziel-Volumes“ die einzelnen Volumes aus, die wiederhergestellt werden sollen. Deaktivieren Sie die Option, wenn Sie ein aufgelistetes Volume nicht wiederherstellen möchten.

HINWEIS: Zum Durchführen der Wiederherstellung muss mindestens ein Volume ausgewählt werden.

c Klicken Sie auf **Fertigstellen**, wenn die Einstellungen korrekt sind.

VORSICHT: Wenn Sie auf Fertigstellen klicken, werden alle vorhandenen Partitionen und Daten auf dem Ziellaufwerk permanent gelöscht und durch den Inhalt des ausgewählten Wiederherstellungspunkts ersetzt (einschließlich Betriebssystem und allen Daten).

Der Assistent zum Wiederherstellen einer Maschine wird geschlossen und die Daten der ausgewählten Volumes des Wiederherstellungspunkts werden auf die Zielmaschine wiederhergestellt.

Fahren Sie mit Schritt 13 fort.

10 Überprüfen Sie auf der Seite „Datenträgerzuordnung - Vorschau“ die Parameter der ausgewählten Wiederherstellungsaktionen. Klicken Sie auf **Fertigstellen**, um die Wiederherstellung durchzuführen.

VORSICHT: Wenn Sie auf Fertigstellen klicken, werden alle vorhandenen Partitionen und Daten auf dem Ziellaufwerk permanent gelöscht und durch den Inhalt des ausgewählten Wiederherstellungspunkts ersetzt (einschließlich Betriebssystem und allen Daten).

11 Wenn die wiederherzustellenden Volumes SQL- oder Microsoft Exchange-Datenbanken enthalten und Sie eine Live-Wiederherstellung durchführen, werden Sie auf der Seite „Datenbankbereitstellungen aufheben“ aufgefordert, die Volumes zu unmounten. Wählen Sie ggf. **Alle Datenbanken nach der Wiederherstellung des Wiederherstellungspunkts wieder bereitstellen** aus, wenn die Datenbanken nach der Wiederherstellung wieder bereitgestellt werden sollen. Klicken Sie anschließend auf **Fertigstellen**.

12 Klicken Sie auf **OK**, um die Statusmeldung mit dem Hinweis zu bestätigen, dass die Wiederherstellung gestartet wurde.

13 Klicken Sie ggf. in der Core Console auf **Ereignisse**, um den Fortschritt der Wiederherstellung zu überwachen. Weitere Informationen finden Sie unter Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen.

Starten einer BMR-Wiederherstellung für Linux

Um eine BMR-Wiederherstellung für Windows-Maschinen durchzuführen, müssen bestimmte Bedingungen erfüllt sein.

Um einen Wiederherstellungspunkt im Core wiederherzustellen, muss eine geeignete Hardware vorhanden sein. Weitere Informationen finden Sie unter Voraussetzungen für eine BMR-Wiederherstellung für Windows-Maschinen.

Die Windows-Zielmaschine für die BMR-Wiederherstellung muss mit dem Start-CD-Image gestartet werden. Weitere Informationen finden Sie unter Verwalten eines Windows-Start-Image.

Zunächst muss der entsprechende Wiederherstellungspunkt ausgewählt werden. Anschließend müssen die Wiederherstellung auf der Hardware eingeleitet und IP-Adresse und temporäres Kennwort, das von der Universal Recovery Console ermittelt wurde, angegeben werden.

Anschließend müssen Sie die Laufwerke zuordnen und die Wiederherstellung starten.

Der Wiederherstellungspunkt enthält die Treiber für die vorherige Hardware. Bei der Durchführung einer Wiederherstellung auf eine unterschiedliche Hardware müssen Sie mit der URC Speichercontrollertreiber in das wiederhergestellte Betriebssystem injizieren, nachdem die Daten auf dem Laufwerk wiederhergestellt wurden, damit das wiederhergestellte Betriebssystem mit der neuen Hardware gestartet werden kann. Nachdem das Betriebssystem nach der Wiederherstellung neu gestartet wurde, können Sie weitere Treiber herunterladen und installieren, die das Betriebssystem für die Interaktion mit der neuen Hardware benötigt.

Führen Sie die folgenden Aufgaben durch, um eine BMR-Wiederherstellung in der AppAssure Core Console zu starten.

- Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung
- Zuordnen von Volumes für eine BMR-Wiederherstellung
- Laden von Treibern mit der Universal Recovery Console
- Injizieren von Treibern auf dem Zielserver

Dies ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen.

Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung

Wenn die Universal Recovery Console auf der Maschine, auf der eine BMR-Wiederherstellung durchgeführt werden soll, zugänglich ist, müssen Sie die den Wiederherstellungspunkt auswählen, der wiederhergestellt werden soll. Navigieren Sie zur Core Console, um den Wiederherstellungspunkt auszuwählen, der geladen werden soll, und geben Sie die Wiederherstellungskonsole als Ziel für die wiederhergestellten Daten an.

HINWEIS: Dieser Schritt ist erforderlich, um eine BMR-Wiederherstellung auf Windows-Maschinen durchzuführen. Für eine BMR-Wiederherstellung auf Linux-Maschinen ist dieser Schritt optional.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Starten einer BMR-Wiederherstellung für Linux.

Bei der Durchführung einer BMR-Wiederherstellung für eine Linux-Maschine in der Core Console ist diese Aufgabe auch ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Starten einer BMR-Wiederherstellung für eine Linux-Maschine über die Befehlszeile.

Führen Sie die folgenden Schritte aus, um einen Wiederherstellungspunkt im Core für die Wiederherstellung auf der physischen oder virtuellen BMR-Zielmaschine auszuwählen.

So wählen Sie einen Wiederherstellungspunkt aus und leiten Sie eine BMR-Wiederherstellung ein

1. Navigieren Sie zur AppAssure Core Console und klicken Sie in der Liste der geschützten Maschinen auf den geschützten Server, für den die BMR-Wiederherstellung durchgeführt werden soll.

   Die Registerkarte „Zusammenfassung“ für die ausgewählte Maschine wird angezeigt.

2. Klicken Sie auf die Registerkarte „Wiederherstellungspunkte“.
3. Klicken Sie in der Liste der Wiederherstellungspunkte auf die rechte spitze Klammer >, um den Wiederherstellungspunkt zu erweitern, der wiederhergestellt werden soll.
4. Klicken Sie in den erweiterten Details für diesen Wiederherstellungspunkt im Menü „Aktionen“ auf **Wiederherstellen**.

   Der Assistent zum Wiederherstellen einer Maschine wird angezeigt.

5. Wählen Sie **Wiederherstellung auf einer beliebigen Zielmaschine mit einer Start-CD** aus.
6. Wählen Sie **Ich habe bereits eine Start-CD für die Zielmaschine** aus.

   Die Authentifizierungsfelder werden verfügbar.

7 Geben Sie die in der folgenden Tabelle beschriebenen Verbindungsinformationen für die Maschine ein.

Tabelle 86.

Textfeld	Beschreibung
IP-Adresse	Die IP-Adresse der Maschine, die wiederhergestellt werden soll. Diese Adresse ist mit der IP-Adresse identisch, die im URC angezeigt wird.
Authentifizierungs-schlüssel	Das jeweilige Kennwort für die Verbindung zum ausgewählten Server. Dieses Kennwort ist mit dem Authentifizierungsschlüssel identisch, der im URC angezeigt wird.

8 Klicken Sie auf **Weiter**.

Wenn die eingegebenen Verbindungsinformationen mit den URC-Informationen übereinstimmen und Core und Zielserver sich gegenseitig einwandfrei im Netzwerk finden, werden die Volumes des ausgewählten Wiederherstellungspunkt geladen und die Seite „Datenträgerzuordnung“ geladen. In diesem Fall müssen Sie als Nächstes Volumes zuordnen.

HINWEIS: Obwohl AppAssure FAT32- und ReFS-Partitionen unterstützt, werden zurzeit lediglich vollständige Wiederherstellung und BMR-Wiederherstellung unterstützt, da es bei ReFS Treibereinschränkungen gibt, sodass Wiederherstellung, VM-Export usw. im Benutzermodus implementiert sind. Wenn ein Core mindestens ein Agent-Volume schützt, das das Dateisystem ReFS enthält, muss die Installation auf einer Maschine mit Windows 8, Windows 8.1, Windows Server 2012 oder Windows Server 2012 R2 erfolgen, da ReFS nativ unterstützt wird. Andernfalls ist die Funktionalität begrenzt und Vorgänge, bei denen beispielsweise ein Volume-Image bereitgestellt werden muss, funktionieren nicht. In diesem Fall werden in der AppAssure Core Console entsprechende Fehlermeldungen angezeigt.

Eine BMR-Wiederherstellung (Bare Metal Restore) der Festplattenkonfiguration für Speicherplätze (eine Funktion von Windows 8.1) wird in diesem Release ebenfalls nicht unterstützt. Details finden Sie im *Dell AppAssure Bereitstellungshandbuch*.

Zuordnen von Volumes für eine BMR-Wiederherstellung

Nachdem die Verbindung zur Universal Recovery Console hergestellt wurde, müssen Sie die im Wiederherstellungspunkt aufgeführten Volumes und die Volumes der Zielhardware zuordnen, damit die Wiederherstellung durchgeführt werden kann.

AppAssure versucht, Volumes automatisch zuzuordnen. Wenn Sie die Standardzuordnung übernehmen, wird die Festplatte in der Zielmaschine bereinigt und neu partitioniert, sodass alle bereits vorhandenen Daten gelöscht werden. Die Zuordnung erfolgt in der Reihenfolge, in der die Volumes im Wiederherstellungspunkt aufgelistet sind, und die Volumes werden den Datenträgern entsprechend der Größe usw. zugewiesen. Ausgehend davon, dass genügend Speicherplatz auf dem Ziellaufwerk ist, ist keine Partitionierung erforderlich, wenn die automatische Datenträgerzuordnung verwendet wird. Ein Datenträger kann von mehreren Volumes genutzt werden. Wenn Sie die Laufwerke manuell zuordnen, müssen Sie beachten, dass Sie einen Datenträger nicht zweimal verwenden können.

Bei einer manuellen Zuordnung muss die neue Maschine vor der Wiederherstellung bereits richtig formatiert sein. Die Zielmaschine muss über eine separate Partition für jedes Volume im Wiederherstellungspunkt verfügen (einschließlich dem für das System reservierten Volume). Weitere Informationen finden Sie unter Starten einer BMR-Wiederherstellung für Linux.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Starten einer BMR-Wiederherstellung für Linux.

Bei der Durchführung einer BMR-Wiederherstellung für eine Linux-Maschine in der Core Console ist diese Aufgabe auch ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Starten einer BMR-Wiederherstellung für Linux.

Führen Sie die folgenden Schritte aus, um ein Volume zuzuordnen.

So ordnen Sie Volumes für eine BMR-Wiederherstellung zu

1 Wenn Volumes automatisch zugeordnet werden sollen, gehen Sie wie folgt vor: Wenn Volumes manuell zugeordnet werden sollen, fahren Sie mit Schritt 2 fort.

   a Wählen Sie auf der Seite „Datenträgerzuordnung“ des Wiederherstellungsassistenten die Registerkarte „Volumes automatisch zuordnen“ aus.

   b Überprüfen Sie im Bereich „Datenträgerzuordnung“ unter „Quell-Volume“, ob das Quell-Volume ausgewählt ist und die entsprechenden Volumes darunter aufgelistet werden sowie ausgewählt sind.

   > **HINWEIS:** Bei einer BMR-Wiederherstellung sollte zumindest das Volume „System-reserviert“ und das System-Volume (normalerweise, aber nicht immer das Volume C:\) wiederhergestellt werden.

   c Deaktivieren Sie die Option unter „Quell-Volume“, wenn Sie ein aufgelistetes Volume nicht wiederherstellen möchten. Zum Durchführen der BMR-Wiederherstellung muss mindestens ein Volume ausgewählt werden.

   d Wählen Sie **Zielfestplatte** aus, wenn der automatisch zugeordnete Zieldatenträger das richtige Ziel-Volume ist, und vergewissern Sie sich, dass alle entsprechenden Volumes ausgewählt sind.

   e Klicken Sie auf **Wiederherstellen** und gehen Sie zu Schritt Schritt 3.

2 Wenn Volumes manuell zugeordnet werden sollen, gehen Sie wie folgt vor:

   a Wählen Sie auf der Seite „Datenträgerzuordnung“ des Wiederherstellungsassistenten die Registerkarte „Volumes manuell zuordnen“ aus.

   > **HINWEIS:** Wenn keine Volumes auf dem Laufwerk der Maschine vorhanden sind, auf der ein BMR-Wiederherstellung durchgeführt wird, können Sie diese Registerkarte nicht anzeigen oder keine Volumes manuell zuordnen.

   b Überprüfen Sie im Bereich „Volume-Zuordnung“ unter „Quell-Volume“, ob das Quell-Volume ausgewählt ist und die entsprechenden Volumes darunter aufgelistet werden sowie ausgewählt sind.

   c Wählen Sie im Dropdown-Menü unter „Ziel“ das gewünschte Ziel für das Ziel-Volume aus, um die BMR-Wiederherstellung des ausgewählten Wiederherstellungspunkts durchzuführen, und klicken Sie dann auf **Wiederherstellen**.

3 Überprüfen Sie im Bestätigungsdialogfeld die Zuordnung des Quell-Volumes im Wiederherstellungspunkt und den Ziel-Volumes für die Wiederherstellung. Klicken Sie auf **Wiederherstellung starten**, um die Wiederherstellung durchzuführen.

> **VORSICHT: Wenn Sie auf Wiederherstellung starten klicken, werden alle vorhandenen Partitionen und Daten auf dem Ziellaufwerk permanent gelöscht und durch den Inhalt des ausgewählten Wiederherstellungspunkts ersetzt (einschließlich Betriebssystem und allen Daten).**

Laden von Treibern mit der Universal Recovery Console

Beim Erstellen einer Start-CD können Sie die erforderlichen Treiber zum ISO-Image hinzufügen. Nach dem Starten der Zielmaschine können Sie Speicher- oder Netzwerktreiber auch in der Universal Recovery Console (URC) laden. Mithilfe dieser Funktion können Sie Treiber hinzufügen, die vergessen wurden und nicht im ISO-Image enthalten sind, aber für eine BMR-Wiederherstellung erforderlich sind.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Starten einer BMR-Wiederherstellung für Linux.

Führen Sie die folgenden Schritte aus, um Treiber mit der URC zu laden.

So laden Sie Treiber mit der Universal Recovery Console

1. Laden Sie die erforderlichen Treiber auf einer Maschine mit einer Internetverbindung herunter und speichern Sie die Treiber auf einem Wechseldatenträger, z. B. auf einem USB-Laufwerk.
2. Entnehmen Sie den Datenträger aus der Maschine und schließen Sie ihn an den Zielserver an, der gestartet werden soll.
3. Klicken Sie in der URC auf dem Zielserver auf der Registerkarte „Konsole“ auf **Treiber laden**.
4. Navigieren Sie im Fenster „Treiber auswählen“ zum Speicherort des Treibers und klicken Sie auf **Öffnen**.
5. Wiederholen Sie die obigen Schritte für jeden Treiber, die Sie laden möchten.

Injizieren von Treibern auf dem Zielserver

Bei der Wiederherstellung auf einer anderen Hardware müssen Sie Speichercontroller-, RAID-, AHCI-, Chipsatz- und andere Treiber injizieren, wenn diese noch nicht auf der Start-CD vorhanden sind. Diese Treiber ermöglichen einen einwandfreien Betrieb aller Geräte des Zielservers im Betriebssystem, sobald das System nach der Wiederherstellung neu gestartet wurde.

Klicken Sie in der Universal Recovery Console auf die Registerkarte „Systeminformationen“, wenn Sie nicht sicher sind, welche Treiber vom Zielserver benötigt werden. Auf dieser Registerkarte werden die gesamte Systemhardware und alle Gerätetypen für den Zielserver angezeigt, auf dem die Wiederherstellung durchgeführt werden soll.

HINWEIS: Der Zielserver enthält automatisch einige generische Windows 7 PE 32-Bit-Treiber, die für viele Systeme ausreichend sind.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Starten einer BMR-Wiederherstellung für Linux.

Führen Sie die folgende Aufgabe durch, um Treiber auf dem Zielserver zu injizieren.

So injizieren Sie Treiber auf dem Zielserver

1. Laden Sie die Treiber von der Website des Serverherstellers herunter und entpacken Sie sie.
2. Komprimieren Sie jeden Treiber mit einem entsprechenden Programm (z. B. WinZip) in eine .zip-Datei und kopieren Sie die Datei auf den Zielserver.
3. Klicken Sie in der Universal Recovery Console auf **Treiberinjektion**.
4. Navigieren Sie im Dateisystem zur komprimierten Treiberdatei und wählen Sie die Datei aus.
5. Klicken Sie auf **Treiber hinzufügen**, wenn Sie in Schritt 3 „Treiberinjektion“ ausgewählt haben. Klicken Sie auf **Öffnen**, wenn Sie in Schritt 3 „Treiber laden“ ausgewählt haben.

   Die ausgewählten Treiber werden injiziert und nach dem Neustart des Zielservers im Betriebssystem geladen.
6. Wiederholen Sie Schritt 3 bis Schritt 5 je nach Bedarf, bis alle Treiber injiziert wurden.

Überprüfen einer BMR-Wiederherstellung

Wenn Sie eine BMR-Wiederherstellung (Bare Metal Restore) durchführen, können Sie den Fortschritt der Wiederherstellung überprüfen. Wenn der Vorgang erfolgreich durchgeführt wurde, können Sie den wiederhergestellten Server starten. In den folgenden Abschnitten finden Sie auch einige Informationen zur Fehlerbehebung, wenn beim Herstellen der Verbindung zur Universal Recovery Console zum Durchführen der Wiederherstellung oder beim Neustart der wiederhergestellten Maschine Probleme auftreten.

Sie können die folgenden Aufgaben durchführen:

- Anzeigen des Fortschritts der Wiederherstellung

- Starten eines wiederhergestellten Zielservers
- Beheben von Universal Recovery Console-Verbindungsproblemen
- Reparieren von Startproblemen

Dies ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen.

Anzeigen des Fortschritts der Wiederherstellung

Führen Sie die folgenden Schritte durch, um den Fortschritt der Datenwiederherstellung aus einem Wiederherstellungspunkt anzuzeigen, die in der AppAssure Core Console eingeleitet wurde (einschließlich BMR-Wiederherstellung).

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Überprüfen einer BMR-Wiederherstellung.

So zeigen Sie den Wiederherstellungsfortschritt an

1. Nachdem die Wiederherstellung aus einem Wiederherstellungspunkt gestartet wurde, können Sie den Fortschritt über das Dropdown-Menü „Aktive Aufgaben“ in der Core Console anzeigen, während die Aufgabe durchgeführt wird.
2. Optional können Sie detaillierte Informationen auf der Registerkarte „Ereignisse“ anzeigen. Weitere Informationen zur Überwachung von AppAssure-Ereignissen finden Sie unter Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen.

Starten eines wiederhergestellten Zielservers

Führen Sie die nachstehend beschriebenen Schritte aus, um den wiederhergestellten Zielserver zu starten.

HINWEIS: Bevor Sie den wiederhergestellten Zielserver starten, sollten Sie überprüfen, ob die Wiederherstellung erfolgreich durchgeführt wurde. Weitere Informationen finden Sie unter Anzeigen des Fortschritts der Wiederherstellung.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Überprüfen einer BMR-Wiederherstellung.

So starten Sie einen wiederhergestellten Zielserver

1. Navigieren Sie wieder zum Zielserver und vergewissern Sie sich, dass die AppAssure Universal Recovery Console aktiv ist.
2. Entnehmen Sie die Start-CD aus dem wiederhergestellten Server (oder trennen Sie den physischen Datenträger mit dem Start-CD-Image).
3. Klicken Sie in der Universal Recovery Console auf der Registerkarte „Konsole“ auf **Neustart**.
4. Geben Sie an, dass das Betriebssystem normal gestartet werden soll.
5. Melden Sie sich bei der Maschine an. Das wiederhergestellte System sollte den im Wiederherstellungspunkt erfassten Zustand aufweisen.

Beheben von Universal Recovery Console-Verbindungsproblemen

Nachstehend finden Sie einige Informationen zum Beheben von Problemen bei Herstellen einer Verbindung zum Start-CD-Image beim Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Überprüfen einer BMR-Wiederherstellung.

Wenn ein Fehler angezeigt wird, dass der Core keine Verbindung zum Remote-Server herstellen konnte, kommen mehrere mögliche Ursachen dafür infrage.

- Vergewissern Sie sich, dass die in der URC angezeigte IP-Adresse und das aktuelle Kennwort mit den Informationen übereinstimmen, die Sie im Dialogfeld „Recovery Console-Instanz“ eingegeben haben.
- Damit der Core den Server erreichen kann, auf dem die Daten wiederhergestellt werden sollen, muss der Core den Server im Netzwerk finden können. Um festzustellen, ob dies möglich ist, können Sie auf dem Core eine Eingabeaufforderung öffnen und einen Ping-Befehl an die IP-Adresse des BMR-Zielservers absetzen. Sie können auch auf dem Zielserver eine Eingabeaufforderung öffnen und einen Ping-Befehl an den AppAssure Core absetzen.
- Überprüfen Sie, ob die Netzwerkadaptereinstellungen von Core und BMR-Zielserver kompatibel sind.

Reparieren von Startproblemen

Führen Sie die folgenden Schritte aus, um Probleme beim Systemstart zu beheben. Bedenken Sie, dass Sie bei der Wiederherstellung auf einer anderen Hardware Speichercontroller-, RAID-, AHCI-, Chipsatz- und andere Treiber injiziert haben müssen, wenn diese noch nicht auf der Start-CD vorhanden sind. Diese Treiber ermöglichen einen einwandfreien Betrieb aller Geräte des Zielservers im Betriebssystem. Weitere Informationen finden Sie unter Injizieren von Treibern auf dem Zielserver.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Überprüfen einer BMR-Wiederherstellung.

Führen Sie die folgenden Schritte durch, um Startproblem des Zielservers zu reparieren.

So reparieren Sie Probleme beim Systemstart

1. Öffnen Sie die Universal Recovery Console, indem Sie erneut die Start-CD laden.
2. Klicken Sie in der Universal Recovery Console auf **Treiberinjektion**.
3. Klicken Sie im Dialogfeld „Treiberinjektion“ auf **Startprobleme reparieren**.

   Die Startparameter im Startdatensatz des Zielservers werden automatisch repariert.
4. Klicken Sie in der Universal Recovery Console auf **Neustart**.

Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen

In AppAssure können Sie eine BMR-Wiederherstellung (Bare Metal Restore) für eine Linux-Maschine durchführen (einschließlich der Wiederherstellung der System-Volumes). Bei der Wiederherstellung einer Linux-Maschine wird ein Rollback auf den Wiederherstellungspunkt des Start-Volumes durchgeführt. Die BMR-Wiederherstellung kann mit dem Befehlszeilenprogramm „aamount“ sowie in der Benutzeroberfläche der Core Console durchgeführt werden.

Um eine BMR-Wiederherstellung für Linux-Maschinen durchzuführen, müssen Sie die folgenden Aufgaben durchführen.

- **Verwalten eines Linux-Start-Image**. Das Start-ISO-Image der Linux Live DVD wird zum Starten des Ziellaufwerks verwendet. Von dort aus können Sie auf die Universal Recovery Console zugreifen, um Sicherungen auf dem Core zu übertragen. Siehe Verwalten eines Linux-Start-Image.
  - Wenn zum Starten der Linux-Zielmaschine ein physischer Datenträger erforderlich ist, müssen Sie weiterhin das ISO-Image auf ein Medium übertragen. Siehe Übertragen desLive DVD ISO-Image auf Datenträger.
  - In allen Fällen müssen Sie das Start-Image im Zielserver laden und den Server vom Start-Image starten. Siehe Laden der Live DVD und Starten der Zielmaschine.

- **Verwalten von Partitionen**. Eventuell müssen Sie Partitionen erstellen oder mounten, damit Sie eine BMR-Wiederherstellung auf einer Linux-Maschine durchführen können. Siehe Verwalten von Linux-Partitionen.
    - Das Linux-System, auf dem eine BMR-Wiederherstellung durchgeführt wird, muss dieselben Partitionen aufweisen wie die Quell-Volumes im Wiederherstellungspunkt. Sie müssen ggf. weitere Partitionen im Zielsystem erstellen. Siehe Erstellen von Partitionen auf dem Ziellaufwerk.
    - Mounten von Partitionen. Wenn Sie eine manuelle BMR-Wiederherstellung durchführen, müssen Sie zuerst Partitionen mounten. Siehe Mounten von Partitionen über die Befehlszeile. Die Schritte zum Mounten von Partitionen sind in der Vorgehensweise zum Durchführen einer BMR-Wiederherstellung von der Befehlszeile enthalten. Siehe Starten einer BMR-Wiederherstellung für eine Linux-Maschine über die Befehlszeile.

      Wenn Sie in der Core Console die automatische Partitionierung für die BMR-Wiederherstellung verwenden, müssen Sie keine Partitionen mounten. AppAssure stellt die Partitionen wieder her, die auch im wiederhergestellten Wiederherstellungspunkt enthalten sind.
- **Starten einer BMR-Wiederherstellung für Linux**. Nachdem die Zielmaschine vom Live DVD-Start-Image gestartet wurde, können Sie die BMR-Wiederherstellung starten. Die jeweils erforderlichen Aufgaben hängen davon ab, ob die Wiederherstellung in der AppAssure-Benutzeroberfläche oder über die Befehlszeile mit dem Dienstprogramm „aamount“ erfolgt. Siehe Starten einer BMR-Wiederherstellung für Linux.
    - Wenn Sie die Core Console verwenden, müssen Sie eine Wiederherstellung aus einem Wiederherstellungspunkt im Core einleiten. Siehe Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung.
    - Wenn Sie die Core Console verwenden, müssen Sie die Volumes auf der Benutzeroberfläche zuordnen. Siehe Zuordnen von Volumes für eine BMR-Wiederherstellung.
    - Bei der Wiederherstellung über die Befehlszeile können Sie ggf. das Dienstprogramm „Screen“ starten, damit die Befehle in der Terminalkonsole übersichtlicher angezeigt werden und die Bedienung erleichtert wird. Weitere Informationen finden Sie unter Starten des Dienstprogramms „Screen“.
    - Wenn Sie „aamount“ verwenden, werden alle Aufgaben über die Befehlszeile ausgeführt. Weitere Informationen finden Sie unter Starten einer BMR-Wiederherstellung für eine Linux-Maschine über die Befehlszeile.
- **Überprüfen einer BMR-Wiederherstellung**. Nachdem die BMR-Wiederherstellung (Bare Metal Restore) gestartet wurde, können Sie den Fortschritt überprüfen und überwachen. Siehe Überprüfen der BMR-Wiederherstellung über die Befehlszeile.
    - Sie können den Fortschritt der Wiederherstellung überwachen. Siehe Anzeigen des Fortschritts der Wiederherstellung.
    - Danach können Sie den wiederhergestellten Server starten. Siehe Starten eines wiederhergestellten Zielservers.
    - Beheben von Fehlern beim BMR. Siehe Beheben von Universal Recovery Console-Verbindungsproblemen und Reparieren von Startproblemen.

Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen

Damit Sie eine BMR-Wiederherstellung (Bare Metal Restore) für eine Linux-Maschine durchführen können, müssen die folgenden Bedingungen und Kriterien erfüllt sein:

- **Vorhandensein von Sicherungen der Maschine, die wiederhergestellt werden soll.** Es muss ein funktionierender AppAssure Core mit Wiederherstellungspunkten des geschützten Servers vorhanden sein, der wiederhergestellt werden soll.

- **Hardware für die Wiederherstellung (neu oder alt, vergleichbar oder unterschiedlich).** Die Zielmaschine muss die Installationsanforderungen für einen Agenten erfüllen. Entsprechende Details finden Sie im *Dell AppAssure Bereitstellungshandbuch*.
- **Live DVD-Start-Image**. Besorgen Sie sich das Linux Live DVD-ISO-Image, das eine startfähige Linux-Version umfasst. Sie können es vom Dell Software-Lizenzportal unter https://licenseportal.com herunterladen. Wenden Sie sich an den Dell AppAssure-Support, wenn Probleme beim Herunterladen der Live DVD auftreten.
- **Image-Datenträger und -Software.** Wenn Sie physische Medien verwenden, müssen Sie über eine leere CD oder DVD sowie über eine Software zum Brennen von Datenträgern oder eine Software zum Erstellen eines ISO-Image verfügen.
- **Kompatible Speichertreiber und Netzwerkadaptertreiber.** Bei der Wiederherstellung auf unterschiedlicher Hardware müssen ggf. kompatible Speichertreiber und Netzwerkadaptertreiber (z. B. RAID, AHCI) für die Zielmaschine sowie Chipsatztreiber für das Zielbetriebssystem vorhanden sein.
- **Speicherplatz und Partitionen je nach Bedarf.** Auf der Zielfestplatte muss genügend Speicherplatz zum Erstellen der Zielpartitionen auf der Zielmaschine für die Quell-Volumes vorhanden sein. Jede Zielpartition muss mindestens so groß sein wie die ursprüngliche Quellpartition.
- **Wiederherstellungspfad.** Geben Sie den Pfad für die Wiederherstellung an (Pfad zum Deskriptor der Gerätedatei). Geben Sie in einem Terminalfenster den Befehl `fdisk` ein, um den Pfad für den Gerätedateideskriptor zu ermitteln.

Verwalten eines Linux-Start-Image

Für eine BMR-Wiederherstellung (Bare Metal Restore) unter Linux ist ein Live DVD-Start-Image erforderlich, das Sie vom Dell Software-Lizenzportal herunterladen können. Mit diesem Image wird die Linux-Zielmaschine gestartet. Abhängig von den jeweiligen Eigenschaften der Umgebung müssen Sie dieses Image u. U. auf ein physisches Medium übertragen (z. B. CD oder DVD). Anschließend müssen Sie das Start-Image virtuell oder physisch laden und den Linux-Server mit dem Start-Image starten.

HINWEIS: Die Live DVD wurde zuvor Live CD genannt.

Sie können die folgenden Aufgaben durchführen:

- Herunterladen eines ISO-Start-Image für Linux
- Übertragen desLive DVD ISO-Image auf Datenträger
- Laden der Live DVD und Starten der Zielmaschine

Das Verwalten eines Linux-Start-Image ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen.

Herunterladen eines ISO-Start-Image für Linux

Bei der Durchführung einer BMR-Wiederherstellung (Bare Metal Restore) für eine Linux-Maschine muss als Erstes das ISO-Image für die Linux Live DVD vom Dell Software-Lizenzportal heruntergeladen werden. Die Live DVD funktioniert mit allen Linux-Dateisystemen, die AppAssure unterstützt. Sie enthält eine startfähige Linux-Version, das Dienstprogramm „Screen“ sowie die AppAssure URC-Schnittstelle (Universal Recovery Console). Bei der AppAssure Universal Recovery Console handelt es sich um eine Umgebung, mit der das Systemlaufwerk oder ein ganzer Server direkt vom AppAssure Core aus wiederhergestellt werden kann.

HINWEIS: Die ISO (International Organization for Standardization) ist eine internationale Organisation von Vertretern aus verschiedenen nationalen Organisationen, die Normen für Dateisysteme festlegt. ISO 9660 ist eine Norm für Dateisysteme, die für optische Datenträger zum Austausch von Daten verwendet wird und mehrere Betriebssysteme unterstützt. Ein ISO-Image ist die Archivdatei oder das Datenträger-Image, das die Daten der einzelnen Sektoren sowie das Dateisystem des Datenträgers enthält.

Sie müssen das jeweilige Live DVD ISO-Image für die verwendete Version von AppAssure herunterladen. Die aktuelle Version der Live DVD steht im Dell Software-Lizenzportal unter https://licenseportal.com zur Verfügung. Wenden Sie sich an den Dell AppAssure Support, wenn Sie eine andere Version benötigen.

HINWEIS: Weitere Informationen zum Dell Software-Lizenzportal finden Sie im *Lizenzportal Benutzerhandbuch* auf der Dokumentationswebsite mit AppAssure-Releaseinformationen und -Handbüchern unter https://support.software.dell.com/appassure/release-notes-guides.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten eines Linux-Start-Image.

Führen Sie die folgenden Schritte aus, um das Live DVD ISO-Image herunterzuladen.

So laden Sie ein ISO-Start-Image für Linux herunter

1. Melden Sie sich beim Dell Software-Lizenzportal unter https://licenseportal.com an.
2. Öffnen Sie den Bereich **Downloads**.
3. Navigieren Sie zu „Linux Based Applications“ und klicken Sie im Abschnitt „Linux Live DVD“ auf **Download**.
4. Speichern Sie das Live DVD ISO-Image. Bei der Wiederherstellung einer virtuellen Maschine können Sie das Image in einem Netzwerkspeicherort speichern und die VM so einrichten, dass sie von einem CD- oder DVD-Laufwerk mit dem ISO-Image gestartet wird.
5. Bei der Wiederherstellung einer physischen Maschine müssen Sie das ISO-Image der Start-CD auf einen CD- oder DVD-Datenträger brennen, mit dem das System gestartet werden kann. Weitere Informationen finden Sie unter Übertragen desLive DVD ISO-Image auf Datenträger.

Übertragen desLive DVD ISO-Image auf Datenträger

Wenn Sie die Linux Live DVD-Datei herunterladen, wird die Datei im angegebenen Pfad als ISO-Image gespeichert. Sie müssen die Linux-Zielmachine vom Live DVD-Image starten können.

Sie können das ISO-Image der Start-CD auf CD- oder DVD-Datenträger brennen.

Beim Start der Maschine mit der Live DVD wird automatisch die Universal Recovery Console gestartet.

Bei einer BMR-Wiederherstellung auf einer virtuellen Maschine ist dieser Schritt nicht erforderlich. Laden Sie das ISO-Image einfach in ein Laufwerk und bearbeiten Sie die Einstellungen der VM so, dass sie von diesem Laufwerk aus gestartet wird.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten eines Linux-Start-Image.

Laden der Live DVD und Starten der Zielmaschine

Nachdem das Live DVD ISO-Image heruntergeladen wurde, müssen Sie die Linux-Maschine mit der neu erstellten Live DVD starten.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten eines Linux-Start-Image.

So laden Sie eine Live DVD und starten Sie die Zielmaschine

1. Navigieren Sie zum neuen Server und laden Sie das Live DVD-Image vom jeweiligen Speicherort. Geben Sie an, dass der Server vom Live DVD-Image gestartet wird.
2. Starten Sie die Maschine.

   Daraufhin werden eine AppAssure Begrüßungsanzeige angezeigt und die Universal Recovery Console gestartet, in der die IP-Adresse sowie das Authentifizierungskennwort für die Maschine angezeigt werden.

HINWEIS: Bei jedem Start der Maschine mit dem Live DVD-Image wird ein neues temporäres Kennwort generiert.

3 Notieren Sie sich die in der Begrüßungsanzeige angezeigte IP-Adresse und das Authentifizierungskennwort. Sie benötigen diese Informationen später bei der Datenwiederherstellung, um sich wieder bei der Konsole anzumelden.

Nachdem die Linux-Zielmaschine mit der Live DVD gestartet wurde, kann vom Core aus eine Verbindung hergestellt und die BMR-Wiederherstellung gestartet werden. Sie haben dazu zwei Möglichkeiten:

- Starten einer Wiederherstellung in der AppAssure Core Console. Weitere Informationen finden Sie unter Starten einer BMR-Wiederherstellung für Linux.
- Starten einer Wiederherstellung über die Befehlszeile mit dem Dienstprogramm „aamount“. Weitere Informationen finden Sie unter Starten einer BMR-Wiederherstellung für eine Linux-Maschine über die Befehlszeile.

Verwalten von Linux-Partitionen

Bei der Durchführung einer BMR-Wiederherstellung muss das Ziellaufwerk, auf dem die Daten wiederhergestellt werden, identische Partitionen wie im wiederhergestellten Wiederherstellungspunkt aufweisen. Sie müssen ggf. Partitionen erstellen, damit diese Anforderung erfüllt wird.

Sie können die Wiederherstellung in der Befehlszeile mit dem Dienstprogramm „aamount“ oder in der AppAssure Core Console starten. Bei einer Wiederherstellung mit der Benutzeroberfläche müssen Sie die Partitionen zuerst mounten.

Sie können die folgenden Aufgaben durchführen:

- Erstellen von Partitionen auf dem Ziellaufwerk
- Formatieren von Partitionen auf dem Ziellaufwerk
- Mounten von Partitionen über die Befehlszeile

Das Verwalten der Linux-Partitionen ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen.

Erstellen von Partitionen auf dem Ziellaufwerk

Bei der Durchführung einer BMR-Wiederherstellung ist das Ziellaufwerk oftmals ein neues Volume, das u. U. nur eine Partition umfasst. Das Laufwerk auf der Zielmaschine muss über eine identische Partitionstabelle wie im Wiederherstellungspunkt verfügen (einschließlich Volume-Größe). Wenn das Ziellaufwerk keine identischen Partitionen aufweist, müssen Sie sie erstellen, bevor die BMR-Wiederherstellung durchgeführt wird. Mit dem Dienstprogramm „fdisk“ können Sie auf dem Ziellaufwerk Partitionen erstellen, die mit den Partitionen des Quelllaufwerks identisch sind.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten von Linux-Partitionen.

So erstellen Sie Partitionen auf dem Ziellaufwerk

1 Optional können Sie das Dienstprogramm „Screen“ starten. Sobald es gestartet wurde, bleibt es bis zum Neustart der Maschine aktiv.

HINWEIS: Weitere Informationen finden Sie unter Starten des Dienstprogramms „Screen“.

2 Geben Sie in der Befehlszeile den folgenden Befehl ein und drücken Sie die **Eingabetaste**, um die vorhandenen Festplattenpartitionen mit Administratorberechtigungen anzuzeigen:

```
sudo fdisk -l
```

Eine Liste aller Volumes wird angezeigt.

Im folgenden Beispiel wird davon ausgegangen, dass das Volume /dev/sda partitioniert werden soll. Ändern Sie den Befehl entsprechend, wenn ein anderes Volume verwendet werden soll (bei älteren Laufwerken wir u. U. /dev/hda angezeigt).

3 Geben Sie den folgenden Befehl ein, um eine neue Startpartition zu erstellen, und drücken Sie die **Eingabetaste**:

```
sudo fdisk /dev/sda
```

4 Geben Sie den folgenden Befehl ein, um eine neue Startpartition zu erstellen, und drücken Sie die **Eingabetaste**:

```
n
```

5 Geben Sie den folgenden Befehl ein, um eine neue Primärpartition zu erstellen, und drücken Sie die **Eingabetaste**:

```
p
```

6 Geben Sie die Partitionsnummer ein, um die Partitionsnummer anzugeben, und drücken Sie die **Eingabetaste**. Um beispielsweise die Partition 1 anzugeben, geben Sie 1 ein und drücken Sie die **Eingabetaste**.

7 Drücken Sie die **Eingabetaste**, um den ersten Sektor zu verwenden (2048).

8 Weisen Sie der Startpartition die gewünschte Größe zu. Geben Sie dazu das Pluszeichen sowie die gewünschte Größe ein und drücken Sie die **Eingabetaste**.

Um der Startpartition beispielsweise eine Größe von 500 MB zuzuweisen, geben Sie den folgenden Befehl ein und drücken Sie dann die **Eingabetaste**:

```
+500M
```

9 Um das Startflag für die Startpartition zu setzen (damit die Partition aktiv und startfähig wird), geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
a
```

10 Um ein Startflag für eine Partition zu setzen, geben Sie die Nummer der Partition ein und drücken Sie die **Eingabetaste**. Um beispielsweise ein Startflag für die Partition 1 zu setzen, geben Sie 1 ein und drücken Sie die **Eingabetaste**.

11 Geben Sie den folgenden Befehl ein, um alle im Dienstprogramm „fdisk“ vorgenommenen Änderungen zu speichern, und drücken Sie die **Eingabetaste**:

```
w
```

Formatieren von Partitionen auf dem Ziellaufwerk

Nachdem die Partitionen auf einem neuen Volume auf dem Ziellaufwerk erstellt wurden, müssen Sie die Partitionen formatieren, damit sie gemounted werden können. Führen Sie die folgenden Schritte aus, wenn diese Situation zutrifft, um Partitionen in den Formaten in Ext3, Ext4 oder XFS zu formatieren.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten von Linux-Partitionen.

So formatieren Sie Partitionen auf dem Ziellaufwerk

1 Optional können Sie das Dienstprogramm „Screen“ starten. Sobald es gestartet wurde, bleibt es bis zum Neustart der Maschine aktiv.

> **HINWEIS:** Weitere Informationen finden Sie unter Starten des Dienstprogramms „Screen“.

2 Geben Sie in der Befehlszeile den folgenden Befehl ein und drücken Sie die **Eingabetaste**, um die vorhandenen Festplattenpartitionen mit Administratorberechtigungen anzuzeigen:

```
sudo fdisk -l
```

Eine Liste aller Volumes wird angezeigt.

Im folgenden Beispiel wird davon ausgegangen, dass die Partition /dev/sda1 formatiert werden soll. Ändern Sie den Befehl entsprechend, wenn ein anderes Volume verwendet werden soll (bei älteren Laufwerken wir u. U. /dev/hda angezeigt).

3 Wählen Sie abhängig vom Format, das für die Zielpartition verwendet werden soll, einen der folgenden Befehle aus:

- Geben Sie den folgenden Befehl ein, um eine Partition im Ext3-Format zu formatieren, und drücken Sie die **Eingabetaste**:

  ```
  sudo mkfs.ext3 /dev/sda1
  ```

- Geben Sie den folgenden Befehl ein, um eine Partition im Ext4-Format zu formatieren, und drücken Sie die **Eingabetaste**:

  ```
  sudo mkfs.ext4 /dev/sda1
  ```

- Geben Sie den folgenden Befehl ein, um eine Partition im XFS-Format zu formatieren, und drücken Sie die **Eingabetaste**:

  ```
  sudo mkfs.xfs /dev/sda1
  ```

Die ausgewählte Partition wird entsprechend formatiert.

4 Wiederholen Sie die oben aufgeführten Schritte, wenn weitere Partitionen formatiert werden müssen.

Mounten von Partitionen über die Befehlszeile

Bei der Durchführung einer BMR-Wiederherstellung mit der AppAssure Core Console müssen Sie zuerst die entsprechenden Partitionen auf der Zielmaschine mounten. Führen Sie dies über die Befehlszeile in der Universal Recovery Console aus.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Verwalten von Linux-Partitionen.

Führen Sie die folgenden Schritte aus, um Partitionen auf der Linux-Maschine zu mounten, bevor eine Wiederherstellung durchgeführt wird.

So mounten Sie Partitionen über die Befehlszeile

1 Geben Sie in der Befehlszeile den folgenden Befehl ein und drücken Sie die **Eingabetaste**, um die vorhandenen Festplattenpartitionen mit Administratorberechtigungen anzuzeigen:

```
sudo fdisk -l
```

Eine Liste aller Volumes wird angezeigt.

2 Formatieren Sie alle Partitionen, die für die Durchführung der BMR-Wiederherstellung im Mountverzeichnis benötigt werden. Diese müssen mit den im Wiederherstellungspunkt enthaltenen Volumes übereinstimmen. Wenn das Volume, das gemountet werden soll, beispielsweise „sda1“ heißt, und das Mountverzeichnis „mnt“ ist, geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

3 Mounten Sie alle Partitionen, die für die Durchführung der BMR-Wiederherstellung benötigt werden, im Mountverzeichnis. Diese müssen mit den im Wiederherstellungspunkt enthaltenen Volumes übereinstimmen. Wenn das Volume, das gemountet werden soll, beispielsweise „sda1“ heißt, und das Mountverzeichnis „mnt“ ist, geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
mount /dev/sda1 /mnt
```

4 Wiederholen Sie Schritt 3, bis alle erforderlichen Volumes gemountet wurden.

Nachdem die Volumes gemountet wurden, können Sie in der AppAssure Core Console eine Wiederherstellung auf die Linux-Zielmaschine durchführen. Siehe Starten einer BMR-Wiederherstellung für Linux.

Starten einer BMR-Wiederherstellung für Linux

Um eine BMR-Wiederherstellung für Linux-Maschinen durchzuführen, müssen bestimmte Bedingungen erfüllt sein.

Um einen Wiederherstellungspunkt im Core wiederherzustellen, muss eine geeignete Hardware vorhanden sein. Weitere Informationen finden Sie unter Voraussetzungen für eine BMR-Wiederherstellung für Linux-Maschinen.

Die Linux-Zielmaschine für die BMR-Wiederherstellung muss mit dem Live DVD-Start-Image gestartet werden. Weitere Informationen finden Sie unter Verwalten eines Linux-Start-Image.

Die Anzahl der Volumes auf der Linux-Maschine, die wiederhergestellt werden soll, muss mit der Anzahl der Volumes im Wiederherstellungspunkt übereinstimmen. Sie müssen außerdem wissen, ob die Wiederherstellung in der AppAssure Core Console oder über die Befehlszeile mit „aamount“ durchgeführt werden soll. Weitere Informationen finden Sie unter Verwalten von Linux-Partitionen.

Bei einer Wiederherstellung über die Benutzeroberfläche der Core Console muss zunächst der entsprechende Wiederherstellungspunkt ausgewählt werden, um eine BMR-Wiederherstellung zu starten. Anschließend müssen die Wiederherstellung auf der Hardware eingeleitet und IP-Adresse und temporäres Kennwort, das von der Universal Recovery Console ermittelt wurde, angegeben werden. Anschließend müssen Sie die Laufwerke zuordnen und die Wiederherstellung starten.

Führen Sie die folgenden Aufgaben durch, um eine BMR-Wiederherstellung in der AppAssure Core Console zu starten.

- Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung
- Zuordnen von Volumes für eine BMR-Wiederherstellung
- Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung

Bei einer Wiederherstellung über die Befehlszeile mit dem Dienstprogramm „aamount“ müssen Sie zuerst die entsprechenden Berechtigungen aktivieren, Volumes mounten, „aamount“ ausführen, Informationen zum Core aus der Liste der Maschinen abrufen, eine Verbindung zum Core herstellen, eine Liste der Wiederherstellungspunkte abrufen, den Wiederherstellungspunkt auswählen, der für die BMR-Wiederherstellung verwendet werden soll, und die Wiederherstellung starten.

Optional können Sie das Dienstprogramm „Screen“ starten.

Führen Sie die folgenden Aufgaben durch, um eine BMR-Wiederherstellung über die Befehlszeile zu starten.

- Starten des Dienstprogramms „Screen“
- Starten einer BMR-Wiederherstellung für eine Linux-Maschine über die Befehlszeile

Dies ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Windows-Maschinen.

Starten des Dienstprogramms „Screen“

Auf der Live DVD befindet sich Screen, ein Dienstprogramm, das beim Start von der Live DVD in der Universal Recovery Console zur Verfügung steht. Screen bietet Benutzern die Möglichkeit, gleichzeitig mehrere Shells über eine einzelne SSH-Sitzung (Secure Shell) oder ein einzelnes Konsolenfenster zu verwalten. Sie können damit eine Aufgabe in einem Terminalfenster durchführen (z. B. gemountete Volumes überprüfen) und parallel dazu einen weitere Shell-Instanz öffnen oder verwenden, um eine andere Aufgabe durchzuführen (z. B. das Dienstprogramm „aamount“ ausführen).

Das Dienstprogramm „Screen“ verfügt über einen eigenen Scrollback-Puffer, der die Möglichkeit bietet, mehr Daten auf dem Bildschirm anzuzeigen, z. B. eine Liste der Wiederherstellungspunkte.

HINWEIS: Dieses Dienstprogramm erleichtert lediglich die Arbeit. Seine Verwendung ist optional.

Das Dienstprogramm „Screen“ wird standardmäßig auf der Maschine gestartet, die mit der Live DVD gestartet wird. Wenn Sie diese Anwendung geschlossen haben, müssen Sie das Dienstprogramm „Screen“ von der Live DVD starten. Gehen Sie dazu folgendermaßen vor.

So starten Sie das Dienstprogramm „Screen“

- Geben Sie im Terminalfenster **screen** ein, wenn die Maschine von der Live DVD gestartet wurde, und drücken Sie die **Eingabetaste**.

  Das Dienstprogramm „Screen“ wird gestartet.

Starten einer BMR-Wiederherstellung für eine Linux-Maschine über die Befehlszeile

Wenn das Live DVD ISO-Image auf der Maschine, auf der die BMR-Wiederherstellung durchgeführt werden soll, verfügbar ist sowie Anzahl und Größe der Volumes von Zielmaschine und Wiederherstellungspunkt, der für die BMR-Wiederherstellung verwendet werden soll, übereinstimmen, können Sie die Wiederherstellung in der Befehlszeile mit dem Dienstprogramm `aamount` starten.

Informationen zum Durchführen einer BMR-Wiederherstellung in der AppAssure Core Console-Benutzeroberfläche finden Sie unter Auswählen eines Wiederherstellungspunkts und Einleiten einer BMR-Wiederherstellung.

HINWEIS: Versuchen Sie dabei nicht, Wiederherstellungspunkte im Ordner „/tmp“ bereitzustellen, da dieser die aavdisk-Dateien enthält.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Starten einer BMR-Wiederherstellung für eine Linux-Maschine über die Befehlszeile.

Führen Sie die folgenden Schritte aus, um einen Wiederherstellungspunkt im Core für die Wiederherstellung auf der physischen oder virtuellen BMR-Zielmaschine auszuwählen.

So führen Sie eine BMR-Wiederherstellung für Linux-Maschinen über die Befehlszeile durch

1. Geben Sie den folgenden Befehl ein, um das AppAssure-Dienstprogramm `aamount` als „root“ auszuführen, und drücken Sie die **Eingabetaste**:

   ```
   sudo aamount
   ```

2. Geben Sie den folgenden Befehl ein, um die geschützten Maschinen aufzulisten, und drücken Sie die **Eingabetaste**:

   ```
   lm
   ```

3. Geben Sie die Verbindungsinformationen für den AppAssure Core ein (siehe Beschreibung in der folgenden Tabelle), wenn Sie dazu aufgefordert werden. Drücken Sie nach jeder Eingabe die **Eingabetaste**:

   Tabelle 87.

Textfeld	Beschreibung	Erforderlich
IP-Adresse oder Hostname des AppAssure Core	Die IP-Adresse oder der Hostname des AppAssure Core.	Ja
Domäne	Die Domäne des AppAssure Core. Diese Eingabe ist optional.	Nein
Benutzer	Der Benutzername für einen Administratorbenutzer im Core.	Ja
Kennwort	Das Kennwort für den Administratorbenutzer im Core.	Ja

Daraufhin wird eine Liste der vom AppAssure Core geschützten Maschinen angezeigt. Die Liste enthält die gefundenen Maschinen mit laufender Zeilennummer, Hostanzeigename oder IP-Adresse und ID-Nummer für die Maschine.

4 Geben Sie den lr-Befehl mit der folgenden Syntax ein, um die Wiederherstellungspunkte für die wiederherzustellende Maschine anzuzeigen, und drücken Sie die **Eingabetaste**:

```
lr <Zeilennummer_der_Maschine>
```

HINWEIS: Sie können in diesem Befehl auch die ID-Nummer der Maschine anstelle der laufenden Zeilennummer angeben.

Daraufhin werden die Basiswiederherstellungspunkte und die inkrementellen Wiederherstellungspunkte für die betreffende Maschine aufgelistet. Die Liste umfasst folgende Informationen:

- Zeilennummer
- Datums- und Uhrzeitangabe
- Alphabetische Liste der Volumes im Wiederherstellungspunkt
- Speicherort des Volumes
- Größe des Wiederherstellungspunkts
- ID-Nummer für das Volume mit einer laufenden Nummer am Ende, die den Wiederherstellungspunkt angibt

5 Geben Sie den folgenden Befehl ein, um den Wiederherstellungspunkt für eine Wiederherstellung auszuwählen, und drücken Sie die **Eingabetaste**:

```
r <ID-Nummer_für_Wiederherstellungspunkt> <Pfad>
```

VORSICHT: Sie müssen darauf achten, dass das System-Volume nicht gemountet ist.

HINWEIS: Beim Start der Maschine mit der Live DVD wird das System-Volume nicht gemountet.

Dieser Befehl stellt das Volume-Image mit der angegebenen ID vom Core im angegebenen Pfad wieder her. Der Pfad für die Wiederherstellung ist der Pfad für den Deskriptor der Gerätedatei und nicht das Bereitstellungsverzeichnis.

HINWEIS: Sie können im Befehl auch die Zeilennummer anstelle der ID-Nummer für den Wiederherstellungspunkt angeben, um den Wiederherstellungspunkt anzugeben. In diesem Fall müssen Sie die Zeilennummer für Agent/Maschine (in der `lm`-Ausgabe), gefolgt von der Zeilennummer des Wiederherstellungspunkts und dem Volume-Buchstaben (aus der alphabetischen Liste der Volumes im Wiederherstellungspunkt) und dahinter den Pfad angeben, z. B.:

```
r <Zeilennummer_für_Maschine> <Zeilennummer_für_Wiederherstellungspunkt>
<Volume-Buchstabe> <Pfad>
```

Geben Sie beispielsweise den folgenden Befehl ein:

```
r 1 24 a /dev/sda1
```

In diesem Befehl ist *<Pfad>* der Dateideskriptor für das eigentliche Volume.

6 Geben Sie **y** für Ja ein, wenn Sie aufgefordert werden, den Vorgang fortzusetzen, und drücken Sie die **Eingabetaste**.

Nachdem die Wiederherstellung gestartet wurde, werden entsprechende Meldungen angezeigt, die Sie über den Status informieren.

HINWEIS: Falls eine Ausnahmemeldung angezeigt wird, finden Sie die zugehörigen Details für die Ausnahme in der Datei „aamount.log“. Die Datei „aamount.log“ befindet sich in /var/log/appassure.

7 Beenden Sie „aamount“, wenn die Wiederherstellung erfolgreich durchgeführt wurde, indem Sie `exit` eingeben und dann die **Eingabetaste** drücken.

8 Als Nächstes wird die Wiederherstellung überprüft. Weitere Informationen finden Sie unter Überprüfen der BMR-Wiederherstellung über die Befehlszeile.

Überprüfen der BMR-Wiederherstellung über die Befehlszeile

Dell empfiehlt, die folgenden Schritte durchzuführen, um eine BMR-Wiederherstellung zu überprüfen, die über die Befehlszeile durchgeführt wurde.

- Durchführen einer Dateisystemprüfung für das wiederhergestellte Volume
- Erstellen startfähiger Partitionen auf der wiederhergestellten Linux-Maschine über die Befehlszeile

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen.

Durchführen einer Dateisystemprüfung für das wiederhergestellte Volume

Wenn Sie eine BMR-Wiederherstellung (Bare Metal Restore) über die Befehlszeile ausführen, sollten Sie eine Dateisystemprüfung für das wiederhergestellte Volume durchführen, um sicherzustellen, dass die aus dem Wiederherstellungspunkt wiederhergestellten Daten nicht beschädigt wurden.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Überprüfen der BMR-Wiederherstellung über die Befehlszeile.

Führen Sie die folgende Aufgabe durch, um eine Dateisystemprüfung für das wiederhergestellte Volume durchzuführen.

So führen Sie eine Dateisystemprüfung für das wiederhergestellte Volume durch

1 Geben Sie in der Befehlszeile in der Universal Recovery Console der wiederhergestellten Linux-Maschine den folgenden Befehl ein, um zu überprüfen, ob die entsprechenden Partitionen gemountet wurden, und drücken Sie die **Eingabetaste**:

```
df
```

2 Wechseln Sie zu Schritt 3, wenn das wiederhergestellte Volume nicht gemountet ist. Geben Sie den folgenden Befehl ein, wenn das wiederhergestellte Volume gemountet ist, um es zu unmounten, und drücken Sie die **Eingabetaste**:

```
umount <Volume>
```

3 Geben Sie den folgenden Befehl ein, um eine Dateisystemprüfung für die wiederhergestellten Volumes auszuführen, und drücken Sie die Eingabetaste:

```
fsck <Volume>
```

Wenn „fsck“ ohne Fehlermeldung beendet wird, ist das Dateisystem in Ordnung.

4 Mounten Sie die entsprechenden Volumes erneut. Geben Sie dazu den Befehl `mount <Volume> <Ordner>` ein und drücken Sie die **Eingabetaste**.

Wenn der Volumepfad beispielsweise „dev/sda1“ und der Ordner, der gemountet werden soll, „mnt“ ist, geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
mount /dev/sda1 /mnt
```

Erstellen startfähiger Partitionen auf der wiederhergestellten Linux-Maschine über die Befehlszeile

Wenn die Dateisystemprüfung des wiederhergestellten Volume keine Fehler ergeben hat, müssen Sie startfähige Partitionen erstellen.

GNU Grand Unified Bootloader (GRUB) ist ein Startladeprogramm, mit dem Administratoren konfigurieren können, welches Betriebssystem bzw. welche Kernel-Konfiguration zum Starten des Systems verwendet wird. Nach einer BMR-Wiederherstellung muss die Konfigurationsdatei für GRUB geändert werden, damit die Maschine die entsprechende UUID (Universally Unique Identifier) für das Stamm-Volume verwendet. Bevor Sie diesen Schritt durchführen, müssen Sie Stamm- und Start-Volumes mounten und die jeweilige UUID ermitteln. Dadurch wird sichergestellt, dass ein Start von der Partition möglich ist.

HINWEIS: Diese Vorgehensweise gilt für Linux-Maschinen mit SLES und CentOS/RHEL, die GRUB1 verwenden. Bei Ubuntu, das GRUB2 verwendet, können Sie GRUB2 mit einem Tool aufrufen und reparieren. Ein Beispiel für ein solches Tool ist das Tool „Boot-Repair“, das unter https://help.ubuntu.com/community/Boot-Repair dokumentiert ist.

Diese Aufgabe ist ein Schritt in Anleitung für eine BMR-Wiederherstellung für Linux-Maschinen. Dieser ist Bestandteil des Prozesses zum Überprüfen der BMR-Wiederherstellung über die Befehlszeile.

Führen Sie die folgende Aufgabe durch, um startfähige Partitionen über die Befehlszeile zu erstellen.

So erstellen Sie startfähige Partitionen auf einer Linux-Maschine über die Befehlszeile

1. Geben Sie in der Befehlszeile in der Universal Recovery Console der wiederhergestellten Linux-Maschine den folgenden Befehl als „root“ ein, um alle Geräte mit dem Dienstprogramm „bsctl“ zuzuordnen:

   ```
   sudo bsctl --attach-to-device /<Pfad des wiederhergestellten Volumes>
   ```

   Wenn der Volumepfad beispielsweise „dev/sda1“ und der Ordner, der gemountet werden soll, „mnt“ ist, geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

   ```
   sudo bsctl --attach-to-device /dev/sda1 mnt
   ```

2. Wiederholen Sie diesen Schritt für jedes wiederhergestellte Volume.
3. Sie müssen zuerst das Stamm-Volume und dann das Start-Volume mounten. Mounten Sie die einzelnen wiederhergestellten Volumes mit den folgenden Befehlen:
   a. Geben Sie den folgenden Befehl ein, um das Stamm-Volume zu mounten, und drücken Sie die **Eingabetaste**:

      ```
      mount /<wiederhergestelltes Stamm-Volume> /mnt
      ```

      Wenn beispielsweise /dev/sda2 das Stamm-Volume ist, geben Sie **mount /dev/sda2 /mnt** ein und drücken Sie die **Eingabetaste**.

   b. Geben Sie den folgenden Befehl ein, um das Start-Volume zu mounten, und drücken Sie die **Eingabetaste**:

      ```
      mount /<wiederhergestelltes Start-Volume> /mnt/boot
      ```

      Wenn beispielsweise /dev/sda1 das Start-Volume ist, geben Sie **mount /dev/sda1 /mnt** ein und drücken Sie die **Eingabetaste**.

      HINWEIS: Bei einigen Systemkonfigurationen kann das Startverzeichnis im Stamm-Volume enthalten sein.

4. Wenn das Volume vergrößert wurde (d. h., das Ziel-Volume auf der neuen Linux-Maschine ist größer als das Volume im Wiederherstellungspunkt), müssen Sie alle vorhandenen Bitmap-Datendateien löschen und neu erstellen (siehe Beschreibung in Schritt 5 bis Schritt 8).

   Fahren Sie mit Schritt 9 fort, wenn Quell- und Ziel-Volume gleich groß sind, um den Bitmap-Speicher zurückzusetzen.

In beiden Situationen müssen Sie sie wie in Schritt 10 beschrieben zuordnen.

VORSICHT: Dieser Schritt muss unbedingt durchgeführt werden, bevor Volumes zugeordnet werden. Wenn Sie ein Volume zuordnen und dann die Datei manuell löschen, kann das Volume beschädigt werden.

5 Geben Sie den folgenden Befehl ein, wenn das Volume vergrößert wurde, um den vorhandenen Datenspeicher zu löschen, und drücken Sie die **Eingabetaste**:

```
rm -rf <Bereitstellungspunkt>/.blksnap/data
```

Wenn das wiederhergestellte Volume beispielsweise in „/mnt/sda1“ gemountet wurde, geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
rm -rf /mnt/sda1/.blksnap/data
```

6 Jetzt müssen Sie den vorhandenen Bitmap-Speicher löschen. Geben Sie dazu den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
rm -rf <Bereitstellungspunkt>/.blksnap/bitmap
```

Wenn das wiederhergestellte Volume beispielsweise in „/mnt/sda1“ gemountet wurde, geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
rm -rf /mnt/sda1/.blksnap/bitmap
```

7 Geben Sie den folgenden Befehl ein, wenn der vorhandene Datenspeicher und der Bitmap-Speicher gelöscht wurden, um den Datenspeicher neu zu erstellen, und drücken Sie die **Eingabetaste**:

```
sudo bsctl --create-data-store <Pfad des wiederhergestellten Stamm-Volumes>
```

Geben Sie beispielsweise den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
sudo bsctl --create-data-store /dev/sda1
```

8 Wiederholen Sie diesen Schritt für den Bitmap-Speicher. Geben Sie dazu den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
sudo bsctl --create-bitmap-store <Pfad des wiederhergestellten Stamm-Volumes>
```

Geben Sie beispielsweise den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
sudo bsctl --create-bitmap-store /dev/sda1
```

9 Geben Sie den folgenden Befehl ein, wenn Quell- und Ziel-Volume gleich groß sind, um den Bitmap-Speicher zurückzusetzen, und drücken Sie die **Eingabetaste**:

```
sudo bsctl --reset-bitmap-store <Pfad des wiederhergestellten Volumes>
```

Geben Sie beispielsweise den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
sudo bsctl --reset-bitmap-store /dev/sda1
```

10 Geben Sie in allen Situationen den folgenden Befehl ein, um die Snapshot-Metadaten der einzelnen wiederhergestellten Volumes zuzuordnen, und drücken Sie die **Eingabetaste**:

```
sudo bsctl --map-bitmap-store <Pfad des wiederhergestellten Volumes>
```

Geben Sie beispielsweise den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
sudo bsctl --map-bitmap-store /dev/sda1
```

11 Vergewissern Sie sich, dass die Geräte zugeordnet wurden, indem Sie **bsctl -l** eingeben und die **Eingabetaste** drücken.

12 Ermitteln Sie die UUID (Universally Unique Identifier) der neuen Volumes mit dem Befehl `blkid`. Geben Sie den folgenden Befehl ein und drücken Sie die **Eingabetaste**:

```
blkid <Volume>
```

HINWEIS: Sie können auch den Befehl `ls -l /dev/disk/by-uuid` verwenden.

13 Ermitteln Sie die UUID von `mount /etc/fstab` und vergleichen Sie sie mit den UUIDs für das Stamm-Volume (Ubuntu und CentOS) sowie für das Start-Volume (CentOS und RHEL), indem Sie den folgenden Befehl eingeben und dann die **Eingabetaste** drücken:

```
less /mnt/etc/fstab
```

14 Ermitteln Sie die UUID von `mount /etc/mtab` und vergleichen Sie sie mit den UUIDs für das Stamm-Volume (Ubuntu und CentOS) sowie für das Start-Volume (CentOS und RHEL), indem Sie den folgenden Befehl eingeben und dann die **Eingabetaste** drücken:

```
less /mnt/etc/mtab
```

15 Bei einer BMR-Wiederherstellung auf einer neuen Festplatte in der Zielmaschine müssen Sie die Swap-Partition in „fstab“ im Stamm-Volume auskommentieren.

16 Die Änderung der fstab- und mtab-Pfade muss auf dem wiederhergestellten Volume erfolgen, nicht auf der Live DVD. Es besteht keine Notwendigkeit, Pfade auf der Live DVD zu ändern. Geben Sie die folgenden Befehle ein, um die Installation von GRUB (Grand Unified Bootloader) vorzubereiten. Drücken Sie nach jedem Befehl die **Eingabetaste**:

```
mount --bind /dev /mnt/dev
```

```
mount --bind /proc /mnt/proc
```

17 Suchen Sie die Datei `grub.conf` im gemounteten Volume und öffnen Sie die Datei in einem Texteditor.

Der Speicherort von „grub.conf“ hängt jeweils von der Betriebssystemversion und der installierten Version von GRUB ab. Die wahrscheinlichsten Speicherorte sind **<Stammpfad>/boot/grub/grub.conf**, **<Stammpfad>/boot/grub/grub.cfg** oder **<Stammpfad>/etc/grub.conf**.

18 Suchen Sie in „grub.conf“ alle Zeilen der Form „root=<Stammgeräte-UUID>“ und setzen Sie die richtige UUID für das Stamm-Volume ein. Aktualisieren Sie ggf. alle Vorkommen mit der richtigen UUID. Sie können auch den Stammgerätepfad verwenden. Wenn der Stammgerätepfad wie in den obigen Beispielen „/dev/sda2“ ist, müssen Sie alle Vorkommen in „root=/dev/sda2“ ändern.

19 Entfernen Sie alle Einträge der Form „rd_LVM_LV=“ in der Datei „grub.conf“, speichern Sie die Datei und beenden Sie den Texteditor.

20 Geben Sie den folgenden Befehl ein, um das Stammverzeichnis zu ändern, und drücken Sie die **Eingabetaste**:

```
chroot /mnt /bin/bash
```

21 Installieren Sie GRUB bei Verwendung von SLES, indem Sie die folgenden Befehle eingeben und nach jedem Befehl die **Eingabetaste** drücken:

```
grub-install.unsupported --recheck /dev/sda
```

```
grub-install.unsupported /dev/sda
```

```
grub-install --recheck /dev/sda
```

```
grub-install /dev/sda
```

22 Installieren Sie GRUB bei anderen Linux-Distributionen, indem Sie den folgenden Befehl eingeben und dann die **Eingabetaste** drücken:

```
grub-install/dev/sda
```

> **HINWEIS:** Wenn GRUB unter SUSE installiert wird, sind keine Parameter erforderlich. Geben Sie einfach den Befehl „grub-install“ ein, um GRUB unter SUSE zu installieren, und drücken Sie die **Eingabetaste**.

23 Nehmen Sie die Live DVD aus dem CD- oder DVD-Laufwerk und starten Sie die Linux-Maschine neu.

Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen

Auf der Registerkarte „Ereignisse“ der Core Console wird ein Protokoll aller Systemereignisse für den AppAssure Core angezeigt. Wenn Sie die Registerkarte „Ereignisse“ für eine ausgewählte Maschine anzeigen, wird ein Protokoll aller Systemereignisse für die betreffende Maschine angezeigt.

Der Inhalt der Registerkarte „Ereignisse“ ist in drei Abschnitte unterteilt: Aufgaben, Benachrichtigungen und Ereignisse, in denen jeweils die entsprechenden Details angezeigt werden.

Sie können festlegen, wie Sie über die verschiedenen Ereignisse benachrichtigt werden möchten, indem Sie Benachrichtigungsgruppen erstellen. Weitere Informationen finden Sie unter Konfigurieren von Benachrichtigungsgruppen.

Führen Sie die folgenden Schritte aus, um Aufgaben, Benachrichtigungen bzw. alle Ereignisse anzuzeigen.

Anzeigen von Aufgaben

Eine Aufgabe ist ein Job, den der AppAssure Core durchführen muss, z. B. die Übertragung von Daten in einer regelmäßig geplanten Sicherung oder die Wiederherstellung aus einem Wiederherstellungspunkt.

Aktive Aufgaben werden im Dropdown-Menü „Aktive Aufgaben“ oben in der Core Console aufgelistet.

Sie können auch alle Aufgaben für den AppAssure Core bzw. alle Aufgaben für eine bestimmte Maschine anzeigen.

So zeigen Sie Aufgaben an

1. Navigieren Sie zur AppAssure Core-Registerkarte „Startseite“, um alle Aufgaben für den AppAssure Core anzuzeigen, und klicken Sie auf die Registerkarte **Ereignisse**.

   Navigieren Sie zur Registerkarte „Ereignisse“ einer Maschine, um alle Aufgaben für eine bestimmte geschützte Maschine anzuzeigen.

2. Um nur Aufgaben anzuzeigen, klicken Sie oben links auf der Seite auf **Aufgaben**.

   Die Liste der Ereignisse wird so gefiltert, dass nur Aufgaben für den Core bzw. für die ausgewählte Maschine angezeigt werden.

3. Optional können Sie die Liste der Aufgaben nach Stichwort, Startdatum und/oder Enddatum filtern. Gehen Sie dazu folgendermaßen vor:

   a. Geben Sie ein Stichwort in das Textfeld „Stichwortsuche“ ein, um nach Stichwort zu filtern.

   b. Geben Sie wie folgt Startdatum und -zeit ein, um nach Startdatum und -zeit zu filtern:

      - Geben Sie im Textfeld „Von“ Datum und Uhrzeit im Format MM/TT/JJJJ HH:MM AM/PM ein. Geben Sie beispielsweise 1/1/2013 8:00 AM ein, wenn die Suche am ersten Tag des Januars im Jahr 2014 um 08:00 Uhr beginnen soll.
      - Klicken Sie auf das Kalender-Widget im Textfeld „Von“ und klicken Sie auf **Jetzt**, um den aktuellen Zeitpunkt auszuwählen.
      - Klicken Sie auf das Kalender-Widget, wählen Sie Datum und Uhrzeit im Kalender und mit den Schiebereglern aus und klicken Sie dann auf **Fertig**.

   c. Um die Liste der angezeigten Aufgaben weiter einzugrenzen, können Sie auch ein Enddatum und eine Endzeit angeben.

   Die Liste der Aufgaben wird sofort abhängig von den ausgewählten Kriterien gefiltert.

4. Optional können Sie die in der Liste angezeigten Aufgaben wie folgt filtern:

   - Klicken Sie auf das Symbol **Aktive Aufgaben**, damit nur aktive Aufgaben angezeigt werden.

- Klicken Sie auf das Symbol **Wartende Aufgaben**, damit nur Aufgaben angezeigt werden, die auf ihre Ausführung warten.
- Klicken Sie auf das Symbol **Abgeschlossene Aufgaben**, damit nur Aufgaben angezeigt werden, die beendet wurden.
- Klicken Sie auf das Symbol **Fehlgeschlagene Aufgaben**, damit nur Aufgaben angezeigt werden, die fehlgeschlagen sind.

5 Wählen Sie ein Format in der Liste aus, um die Liste der Aufgaben zu exportieren, und klicken Sie auf **Bericht exportieren...**.

Sie können die folgenden Formate für den Export auswählen:

Tabelle 88.

Format	Beschreibung
PDF	Portable Document Format
XLS	Arbeitsmappe im Format von Excel 1997 - 2003
XLSX	Excel-Arbeitsmappe
RTF	Rich Text Format
CSV	Werte mit Kommas als Trennzeichen

6 Klicken Sie auf das Symbol **Jobdetails** für eine Aufgabe, um ein neues Fenster mit Aufgabendetails zu öffnen. Dazu gehören:

- Startzeit
- Endzeit
- Status
- Abgelaufene Zeit
- Fortschritt
- Geschwindigkeit
- Arbeit, gesamt (Prozentsatz erledigt)
- Untergeordnete Aufgaben (sofern zutreffend)

Anzeigen von Benachrichtigungen

Eine Benachrichtigung bezieht sich auf eine Aufgabe oder ein Ereignis. Benachrichtigungen umfassen Fehler, Warnungen und Informationen.

Sie können alle Benachrichtigungen für den AppAssure Core bzw. alle Benachrichtigungen für eine bestimmte Maschine anzeigen.

So zeigen Sie Benachrichtigungen an

1 Navigieren Sie zur AppAssure Core-Registerkarte „Startseite“, um alle Benachrichtigungen für den AppAssure Core anzuzeigen, und klicken Sie auf die Registerkarte **Ereignisse**.

Navigieren Sie zur Registerkarte „Ereignisse“ einer Maschine, um alle Benachrichtigungen für eine bestimmte geschützte Maschine anzuzeigen.

2 Um nur Benachrichtigungen anzuzeigen, klicken Sie oben links auf der Seite auf **Benachrichtigungen**.

Die Liste der Ereignisse wird so gefiltert, dass nur Benachrichtigungen für den Core bzw. für die ausgewählte Maschine angezeigt werden.

3 Wenn Sie alle Benachrichtigungen löschen möchten, können Sie ggf. auf **Alle schließen** klicken.

Anzeigen aller Ereignisse

Sie können alle Ereignisse für den AppAssure Core bzw. alle Ereignisse für eine bestimmte Maschine anzeigen.

So zeigen Sie Ereignisse an

1. Navigieren Sie zur AppAssure Core-Registerkarte **Startseite**, um alle Ereignisse für den AppAssure Core anzuzeigen, und klicken Sie auf die Registerkarte **Ereignisse**.

   Navigieren Sie zur Registerkarte „Ereignisse“ einer Maschine, um alle Ereignisse für eine bestimmte geschützte Maschine anzuzeigen.

2. Um alle Ereignisse anzuzeigen, klicken Sie oben links auf der Seite auf **Ereignisse**.

   Für den Core bzw. die ausgewählte Maschine werden alle Ereignisse angezeigt.

4

Schützen von Server-Clustern

In diesem Kapitel ist beschrieben, wie Sie mit AppAssure Informationen in Microsoft SQL Server- oder Exchange Server-Clustern schützen können. Folgende Themen werden behandelt:

- Informationen zum Schützen von Server-Clustern in AppAssure
- Schützen eines Clusters
- Schützen von Knoten in einem Cluster
- Ändern der Einstellungen für Cluster-Knoten
- Anleitung zum Konfigurieren von Cluster-Einstellungen
- Konvertieren eines geschützten Cluster-Knotens in einen Agenten
- Anzeigen von Informationen für Server-Cluster
- Verwenden von Cluster-Wiederherstellungspunkten
- Verwalten von Snapshots für einen Cluster
- Aufheben der Bereitstellung lokaler Wiederherstellungspunkte
- Durchführen einer Wiederherstellung für Cluster und Cluster-Knoten
- Replizieren von Cluster-Daten
- Aufheben des Clusters-Schutzes
- Aufheben des Schutzes von Cluster-Knoten
- Anzeigen eines Cluster- oder Knotenberichts

Informationen zum Schützen von Server-Clustern in AppAssure

In AppAssure basiert der Schutz von Server-Clustern auf den AppAssure Agenten, die auf den einzelnen Cluster-Knoten installiert sind (d. h. auf den einzelnen Maschinen im Cluster), und dem AppAssure Core, der diese Agenten so schützt, als ob es sich um eine einzige Maschine handeln würde.

Sie können einen AppAssure Core problemlos zum Schützen und Verwalten eines Clusters konfigurieren. In der Core Console ist ein Cluster als separate Einheit organisiert, die einen „Container“ bildet, in dem die zugehörigen Knoten enthalten sind. Im linken Navigationsbereich werden beispielsweise unter dem Menü „Geschützte Maschinen“ die geschützten Cluster aufgelistet. Direkt unter jedem Cluster werden die zugehörigen Knoten oder Agent-Maschinen angezeigt. Dabei handelt es sich jeweils um eine geschützte Maschine, auf der die AppAssure Agent-Software installiert ist. Wenn Sie auf den Cluster klicken, wird die entsprechende Registerkarte in der Core Console angezeigt.

Auf der Core- und der Cluster-Ebene können Sie Informationen zum Cluster anzeigen, z. B. die Liste der zugehörigen Knoten und die freigegebenen Volumes. Ein Cluster wird in der Core Console auf der Registerkarte „Maschinen“ angezeigt. Sie können die Ansicht (mithilfe von „Ein-/Ausblenden“) umschalten, um die Knoten im Cluster anzuzeigen. Auf der Cluster-Ebene können Sie auch die entsprechenden Exchange- und SQL-Cluster-Metadaten für die Knoten im Cluster anzeigen. Sie können Einstellungen für den gesamten Cluster und die freigegebenen Volumes in diesem Cluster angeben oder zu einem einzelnen Knoten (Maschine) im Cluster navigieren, um die Einstellungen nur für diesen Knoten und die zugehörigen Volumes konfigurieren.

Unterstützte Anwendungen und Cluster-Typen

Um Cluster ordnungsgemäß zu schützen, muss der AppAssure Agent auf allen Maschinen/Knoten im Cluster installiert sein. AppAssure unterstützt die Anwendungsversionen und Cluster-Konfigurationen, die in der folgenden Tabelle aufgeführt sind.

Tabelle 89.

Anwendung	Anwendungsversion und zugehörige Cluster-Konfiguration	Windows-Failover-Cluster
Microsoft Exchange Server	2007 Einzelkopiecluster (SCC) 2007 Fortlaufende Clusterreplikation (CCR)	2003, 2008, 2008 R2
	2010 Datenbankverfügbarkeitsgruppe (DAG)	2008, 2008 R2
	2013 Datenbankverfügbarkeitsgruppe (DAG)	2008 R2 SP1, 2012, 2012 R2
Microsoft SQL Server	2005	2003, 2008, 2008 R2
	2008, 2008 R2 Einzelkopiecluster (SCC)	2003, 2008, 2008 R2, 2012, 2012 R2
	2012, 2014 Einzelkopiecluster (SCC)	2008, 2008 R2, 2012, 2012 R2
	2012, 2014 Verfügbarkeitsgruppen	Server 2012, 2012 R2

Zu den unterstützten Datenträgertypen gehören:

- GPT-Datenträger (GUID-Partitionstabelle) mit einer Kapazität von mehr als 2 TB.
- Basisdatenträger

Zu den unterstützten Bereitstellungstypen gehören:

- Freigegebene Laufwerke, die als Laufwerksbuchstaben angebunden sind (z. B. D:)
- Einfache dynamische Volumes auf einem einzelnen physischen Datenträger (keine Stripeset-Volumes, gespiegelte Volumes oder übergreifende Volumes)
- Freigegebene Laufwerke, die als Bereitstellungspunkte angebunden sind

Begrenzte Unterstützung für freigegebene Clustervolumes.

AppAssure 5 unterstützt native Sicherungen von freigegebenen Clustervolumes nur auf Windows 2008 R2-Agenten.

- Die Unterstützung für freigegebene Clustervolumes ist derzeit auf Agenten beschränkt, die Windows 2008 R2 verwenden.
- Bei anderen Betriebssystemen kann der Agentendienst auf allen Knoten in einem Cluster ausgeführt werden und der Cluster kann als Cluster im AppAssure Core geschützt werden. Freigegebene Clustervolumes werden jedoch nicht in der Core Console angezeigt und können nicht geschützt werden. Alle lokalen Datenträger (z. B. das Betriebssystemvolume) können geschützt werden.

Die folgende Tabelle veranschaulicht die derzeitige Unterstützung im AppAssure 5 Core für freigegebene Clustervolumes.

Tabelle 90. Kompatibilität für freigegebene Clustervolumes in AppAssure 5

Unterstützung von freigegebenen Clustervolumes in AppAssure 5	Schutz, Replikation, Rollup, Archivbereitstellung		Rollback/Wiederherstellung von freigegebenen Clustervolumes		Virtueller Export in freigegebene Hyper-V-Clustervolumes	
AppAssure-Version	5.3	5.4	5.3	5.4	5.3	5.4
Windows 2008 R2	Ja	Ja	Nein	Ja	Ja	Ja

Tabelle 90. Kompatibilität für freigegebene Clustervolumes in AppAssure 5

Unterstützung von freigegebenen Clustervolumes in AppAssure 5	Schutz, Replikation, Rollup, Archivbereitstellung		Rollback/Wiederherstellung von freigegebenen Clustervolumes		Virtueller Export in freigegebene Hyper-V-Clustervolumes	
Windows 2012	Nein	Nein	Nein	Nein	Nein	Nein
Windows 2012 R2	Nein	Nein	Nein	Nein	Nein	Nein

Schützen eines Clusters

In diesem Thema wird beschrieben, wie Sie einen Cluster in AppAssure unter Schutz stellen. Wenn Sie ein Cluster unter Schutz stellen, müssen Sie den Hostnamen oder die IP-Adresse des Clusters, die Cluster-Anwendung oder einen Cluster-Knoten (Cluster-Maschine) angeben, auf dem der AppAssure Agent installiert ist.

HINWEIS: Die Snapshots der Daten, die von den geschützten Knoten erfasst werden, werden In einem Repository gespeichert. Damit Sie Daten im Cluster schützen können, müssen Sie mindestens ein Repository erstellen, das dem AppAssure Core zugewiesen ist.

Weitere Informationen zum Einrichten von Repositorys finden Sie unter Informationen zu Repositorys.

So schützen Sie einen Cluster

1 Navigieren Sie in der Core Console zur Registerkarte „Startseite“ und klicken Sie auf die Schaltfläche **Cluster schützen**.

2 Geben Sie im Dialogfeld „Mit Cluster verbinden“ die folgenden Informationen ein und klicken Sie dann auf **Verbinden**.

Tabelle 91.

Textfeld	Beschreibung
Host	Der Hostname oder die IP-Adresse des Clusters, die Cluster-Anwendung oder ein Cluster-Knoten.
Port	Die Portnummer der Maschine, auf der der AppAssure Core mit dem Agenten kommuniziert. Die Standardportnummer ist 8006.
Benutzername	Der Benutzername des Domänenadministrators für die Verbindung zu dieser Maschine, z. B. domain_name\administrator oder administrator@domain_name.com **HINWEIS:** Der Domänenname muss angegeben werden. Mit dem Benutzernamen eines lokalen Administrators können Sie keine Verbindung zum Cluster herstellen.
Kennwort	Das Kennwort, das für die Verbindung zu dieser Maschine verwendet wird.

3 Wählen Sie im Dialogfeld „Cluster schützen“ ein Repository für diesen Cluster aus.

4 Um den Cluster mit den Standardeinstellungen zu schützen, wählen Sie die entsprechenden Knoten aus und klicken Sie auf **Schützen**.

HINWEIS: Die Standardeinstellungen stellen sicher, dass alle Volumes über einen Zeitplan alle 60 Minuten geschützt werden.

5 Gehen Sie folgendermaßen vor, um benutzerdefinierte Einstellungen für den Cluster einzugeben (z. B. um den Schutzzeitplan für die freigegebenen Volumes anzupassen):

a Klicken Sie auf **Einstellungen**.

b Wählen Sie im Dialogfeld „Volumes“ die zu schützenden Volumes aus und klicken Sie auf **Bearbeiten**.

c Wählen Sie im Dialogfeld „Schutzzeitplan“ eine der in der folgenden Tabelle beschriebenen Zeitplanoptionen zum Schützen der Daten aus.

Tabelle 92.

Textfeld	Beschreibung

Intervall	Sie haben folgende Auswahlmöglichkeiten:
	• **Wochentag.** Um Daten in einem bestimmten Zeitabstand zu schützen, wählen Sie **Intervall** und dann eine der folgenden Optionen aus:
	  • Wenn Sie anpassen möchten, wann Daten in Spitzenauslastungszeiten geschützt werden sollen, können Sie eine Startzeit, eine Endzeit sowie ein Intervall angeben.
	  • Um Daten in Zeiten mit geringer Auslastung zu schützen, aktivieren Sie das Kontrollkästchen **Während Nebenzeiten schützen**, und wählen Sie ein Schutzintervall aus.
	• **Wochenenden.** Wenn Daten auch an den Wochenenden geschützt werden sollen, aktivieren Sie das Kontrollkästchen **An Wochenenden schützen**, und wählen Sie ein Intervall aus.

Täglich	Wenn die Daten täglich geschützt werden sollen, wählen Sie die Option **Täglich** und dann für „Schutzzeit“ die Zeit aus, zu der der Schutz der Daten gestartet werden soll.
Kein Schutz	Um den Schutz für dieses Volume zu entfernen, wählen Sie die Option **Kein Schutz** aus.

6 Klicken Sie auf **Speichern**, nachdem Sie alle notwendigen Änderungen vorgenommen haben.

7 Wählen Sie einen Knoten aus, um angepasste Einstellungen für einen Knoten im Cluster einzugeben, und klicken Sie dann auf den Link **Einstellungen** neben dem Knoten.

- Wiederholen Sie Schritt 5 um den Schutzzeitplan zu bearbeiten.

Weitere Informationen zum Anpassen von Knoten finden Sie unter Schützen von Knoten in einem Cluster.

8 Klicken Sie im Dialogfeld „Cluster schützen“ auf **Schützen**.

Schützen von Knoten in einem Cluster

In diesem Thema wird beschrieben, wie Sie die Daten auf einem Cluster-Knoten oder einer Maschine schützen, auf der ein AppAssure Agent installiert ist. Wenn Sie einen Knoten unter Schutz stellen, müssen Sie den Knoten in der Liste der verfügbaren Knoten auswählen und den Hostnamen, den Benutzernamen und das Kennwort des Domänenadministrators angeben.

So schützen Sie Knoten in einem Cluster

1 Navigieren Sie in der AppAssure Core Console zu dem Cluster, den Sie schützen möchten, nachdem Sie einen Cluster hinzugefügt haben.

Die Registerkarte „Zusammenfassung“ für den ausgewählten Cluster wird angezeigt.

2 Klicken Sie auf die Registerkarte „Geschützte Knoten“ und wählen Sie dann im Menü **Aktionen** die Option **Cluster-Knoten schützen** aus.

3 Geben Sie im Dialogfeld „Cluster-Knoten schützen“ die folgenden Informationen an und klicken Sie anschließend auf **Verbinden**, um die Maschine oder den Knoten hinzuzufügen.

Tabelle 93.

Textfeld	Beschreibung
Host	Eine Dropdown-Liste mit den Knoten, die im Cluster geschützt werden können.
Port	Die Portnummer, über die der AppAssure Core mit dem Agenten auf dem Knoten kommuniziert.
Benutzername	Der Benutzername des Domänenadministrators für die Verbindung zu diesem Knoten , z. B. example_domain\administrator oder administrator@example_domain.com.
Kennwort	Das Kennwort, das für die Verbindung zu dieser Maschine verwendet wird.

4 Klicken Sie auf **Schützen**, um die betreffende Maschine mit den Standardschutzeinstellungen zu schützen.

HINWEIS: Die Standardeinstellungen stellen sicher, dass alle Volumes der Maschine über einen Zeitplan alle 60 Minuten geschützt werden.

5 Um angepasste Einstellungen für diese Maschine einzugeben (z. B. Anzeigename ändern, Verschlüsselung hinzufügen oder den Schutzzeitplan anpassen), klicken Sie auf **Erweiterte Optionen anzeigen**.

6 Bearbeiten Sie die in der folgenden Tabelle beschriebenen Einstellungen je nach Bedarf.

Tabelle 94.

Textfeld	Beschreibung
Anzeigename	Geben Sie einen neuen Namen für die Maschine ein, der in der Core Console angezeigt werden soll.
Repository	Wählen Sie das Repository im AppAssure Core aus, in dem die Daten für diese Maschine gespeichert werden sollen.
Verschlüsselung	Geben Sie an, ob die Daten der einzelnen Volumes dieser Maschine verschlüsselt werden sollen, die in dem Repository gespeichert werden. **HINWEIS:** Die Verschlüsselungseinstellungen für ein Repository werden auf der Registerkarte „Konfiguration“ in der AppAssure Core Console definiert.
Zeitplan	Wählen Sie eine der folgenden Optionen aus. • Alle Volumes mit Standardzeitplan schützen • Bestimmte Volumes mit benutzerdefiniertem Zeitplan schützen Wählen Sie anschließend unter „Volumes“ ein Volume aus und klicken Sie auf **Bearbeiten**. Weitere Informationen zum Festlegen von angepassten Intervallen finden Sie in Schritt 5 unter Schützen eines Clusters.

Ändern der Einstellungen für Cluster-Knoten

Nachdem Sie Cluster-Knoten unter Schutz gestellt haben, können Sie einfach grundlegende Konfigurationseinstellungen für die betreffenden Maschinen oder Knoten (z. B. Anzeigename, Hostname usw.), Schutzeinstellungen (z. B. Schutzzeitplan für lokale Volumes auf der Maschine ändern, Volumes hinzufügen oder entfernen und den Schutz vorübergehend deaktivieren) usw. ändern.

Um die Einstellungen für Cluster-Knoten zu ändern, müssen Sie folgende Schritte ausführen:

1 Navigieren Sie in der AppAssure Core Console zum Cluster mit dem Knoten, der geändert werden soll, und wählen Sie die betreffende Maschine (Knoten) aus.

2 Informationen zum Bearbeiten und Anzeigen von Konfigurationseinstellungen finden Sie unter Konfigurieren von Benachrichtigungsgruppen für Systemereignisse.

3 Informationen zum Konfigurieren von Benachrichtigungsgruppen für Systemereignisse finden Sie unter Anzeigen und Ändern von Konfigurationseinstellungen.

4 Informationen zum Anpassen von Aufbewahrungsrichtlinieneinstellungen finden Sie unter Anpassen der Aufbewahrungsrichtlinieneinstellungen für einen Agenten.

5 Informationen zum Bearbeiten des Schutzzeitplans finden Sie unter Ändern von Schutzzeitplänen.

6 Informationen zum Bearbeiten der Übertragungseinstellungen finden Sie unter Ändern der Übertragungseinstellungen.

Anleitung zum Konfigurieren von Cluster-Einstellungen

Die Anleitung zum Konfigurieren von Cluster-Einstellungen umfasst die folgenden Aufgaben:

- **Ändern der Cluster-Einstellungen.** Weitere Informationen zum Ändern der Cluster-Einstellungen finden Sie unter Ändern der Cluster-Einstellungen.
- **Konfigurieren der Benachrichtigungen für Cluster-Ereignisse.** Weitere Informationen zum Konfigurieren der Benachrichtigungen für Cluster-Ereignisse finden Sie unter Konfigurieren der Benachrichtigungen für Cluster-Ereignisse.
- **Ändern der Cluster-Aufbewahrungsrichtlinie.** Weitere Informationen zum Ändern der Cluster-Aufbewahrungsrichtlinie finden Sie unter Bearbeiten der Cluster-Aufbewahrungsrichtlinie.
- **Ändern der Cluster-Schutzzeitpläne.** Weitere Informationen zum Ändern der Cluster-Schutzzeitpläne finden Sie unter Ändern der Cluster-Schutzzeitpläne.
- **Ändern der Cluster-Übertragungseinstellungen.** Weitere Informationen zum Ändern der Cluster-Übertragungseinstellungen finden Sie unter Ändern der Cluster-Übertragungseinstellungen.

Ändern der Cluster-Einstellungen

Nachdem Sie einen Cluster hinzugefügt haben, können Sie grundlegende Einstellungen (z. B. den Anzeigenamen), Schutzeinstellungen (z. B. Schutzzeitpläne, Volumes hinzufügen oder entfernen sowie Schutz vorübergehend deaktivieren) usw. leicht ändern.

So ändern Sie Cluster-Einstellungen

1 Navigieren Sie in der AppAssure Core Console zu dem Cluster, den Sie ändern möchten.

2 Klicken Sie auf die Registerkarte „Konfiguration“.

Die Seite „Einstellungen“ wird angezeigt.

3 Klicken Sie auf **Bearbeiten**, um die in der folgenden Tabelle beschriebenen Cluster-Einstellungen zu bearbeiten.

Tabelle 95.

Textfeld	Beschreibung
Anzeigename	Geben Sie einen Anzeigenamen für den Cluster ein. Der Name für den Cluster wird in der AppAssure Core Console angezeigt. Standardmäßig ist das der Hostname für den Cluster. Sie können ihn bei Bedarf in einen aussagekräftigeren Namen ändern.

Tabelle 95.

Textfeld	Beschreibung
Repository	Geben Sie das Core-Repository für den Cluster ein. HINWEIS: Wenn für diesen Cluster bereits Snapshots erstellt wurden, ist diese Einstellung hier nur zu Informationszwecken aufgeführt und kann nicht bearbeitet werden.
Verschlüsselungs-schlüssel	In diesem Feld können Sie bei Bedarf einen Verschlüsselungsschlüssel bearbeiten und auswählen. Damit können Sie angeben, ob die Daten der einzelnen Volumes dieser Maschine verschlüsselt werden sollen, die in dem Repository gespeichert werden.

Konfigurieren der Benachrichtigungen für Cluster-Ereignisse

Sie können konfigurieren, wie Systemereignisse für den Cluster gemeldet werden, indem Sie Benachrichtigungsgruppen erstellen. Diese Ereignisse können Systembenachrichtigungen oder -fehler sein. Führen Sie die folgenden Schritte aus, um Benachrichtigungsgruppen für Ereignisse zu konfigurieren.

So konfigurieren Sie Benachrichtigungen für Cluster-Ereignisse.

1 Navigieren Sie in der AppAssure Core Console zu dem Cluster, den Sie ändern möchten.

2 Klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Ereignisse**.

3 Wählen Sie eine der in der folgenden Tabelle beschriebenen Optionen aus.

Tabelle 96.

Option	Beschreibung
Benachrichtigungseinstellungen von Core verwenden	Mit dieser Option werden die Einstellungen angewendet, die vom zugehörigen Core verwendet werden. • Klicken Sie auf **Übernehmen**, und führen Sie dann Schritt 5 durch.
Benutzerdefinierte Benachrichtigungseinstellungen verwenden	Mit dieser Option können Sie benutzerdefinierte Einstellungen konfigurieren. • Fahren Sie mit Schritt 4 fort.

4 Gehen Sie folgendermaßen vor, wenn Sie „Benutzerdefinierte Benachrichtigungseinstellungen verwenden“ ausgewählt haben:

a Klicken Sie auf **Gruppe hinzufügen**, um eine neue Benachrichtigungsgruppe zum Senden einer Liste der Systemereignisse hinzuzufügen.

Das Dialogfeld „Benachrichtigungsgruppe hinzufügen“ wird geöffnet.

b Fügen Sie die in der folgenden Tabelle beschriebenen Benachrichtigungsoptionen hinzu.

Tabelle 97.

Textfeld	Beschreibung
Name	Geben Sie einen Namen für die Benachrichtigungsgruppe ein.
Beschreibung	Geben Sie eine Beschreibung für die Benachrichtigungsgruppe ein.

Tabelle 97.

Textfeld	Beschreibung
Ereignisse aktivieren	Wählen Sie die Ereignisse für die Benachrichtigung aus, z. B. Cluster. Sie können auch den gewünschten Typ auswählen: • Fehler • Warnung • Info HINWEIS: Bei der Auswahl eines bestimmten Typs werden die entsprechenden Ereignisse standardmäßig automatisch aktiviert. Bei Auswahl von „Warnung“ werden beispielsweise die folgenden Ereignisse aktiviert: Anfügbarkeit, Jobs, Lizenzierung, Archiv, Core-Dienst, Export, Schutz, Replikation und Rollback.
Benachrichtigungs-optionen	Wählen Sie aus, wie Benachrichtigungen verarbeitet werden sollen. Sie können zwischen den folgenden Optionen wählen: • **Per E-Mail benachrichtigen**. Geben Sie in den Textfeldern „An“, „CC“ und „BCC“ die E-Mail-Adressen an, an die die Ereignisse gesendet werden sollen. • **Über Windows-Ereignisprotokoll benachrichtigen**. Das Windows-Ereignisprotokoll steuert die Benachrichtigung. • **Über syslogd benachrichtigen.** Geben Sie den Hostnamen und Port an, an den die Ereignisse gesendet werden sollen.

c Klicken Sie auf **OK**, um Ihre Änderungen zu speichern, und anschließend auf **Übernehmen**.

5 Um eine vorhandene Benachrichtigungsgruppe zu bearbeiten, klicken Sie neben einer Benachrichtigungsgruppe in der Liste auf **Bearbeiten**.

Das Dialogfeld „Benachrichtigungsgruppe bearbeiten“ wird angezeigt, in dem Sie die Einstellungen bearbeiten können.

Bearbeiten der Cluster-Aufbewahrungsrichtlinie

Die Aufbewahrungsrichtlinie für einen Cluster gibt an, wie lange die Wiederherstellungspunkte für die freigegebenen Volumes im Cluster im Repository gespeichert werden. Aufbewahrungsrichtlinien werden für die Aufbewahrung von Sicherungs-Snapshots über längere Zeiträume sowie zur Unterstützung bei der Verwaltung dieser Sicherungs-Snapshots verwendet. Eine Aufbewahrungsrichtlinie wird durch einen Rollup-Prozess umgesetzt, der Sie beim Festlegen des Ablaufs und beim Löschen alter Sicherungen unterstützt.

So ändern Sie die Cluster-Aufbewahrungsrichtlinie

1 Navigieren Sie in der AppAssure Core Console zu dem Cluster, den Sie ändern möchten.

2 Klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Aufbewahrungsrichtlinie**.

3 Wählen Sie eine der Optionen in der folgenden Tabelle aus.

Tabelle 98.

Option	Beschreibung
Standard-Aufbewahrungsrichtlinie von Core verwenden	Mit dieser Option werden die Einstellungen angewendet, die vom zugehörigen Core verwendet werden. • Klicken Sie auf **Übernehmen**.
Benutzerdefinierte Aufbewahrungsrichtlinie verwenden	Mit dieser Option können Sie benutzerdefinierte Einstellungen konfigurieren.

HINWEIS: Befolgen Sie die Anweisungen für das Einrichten einer benutzerdefinierten Aufbewahrungsrichtlinie (siehe Beschreibung in Anpassen der Aufbewahrungsrichtlinieneinstellungen für einen Agenten), wenn Sie „Benutzerdefinierte Benachrichtigungseinstellungen verwenden“ ausgewählt haben.

Ändern der Cluster-Schutzzeitpläne

In AppAssure können Sie die Schutzzeitpläne nur ändern, wenn das Cluster freigegebene Volumes umfasst.

So ändern Sie Cluster-Schutzzeitpläne

1. Navigieren Sie in der AppAssure Core Console zu dem Cluster, den Sie ändern möchten, und wählen Sie den Cluster aus.
2. Befolgen Sie die Anweisungen zum Ändern von Schutzeinstellungen (siehe Beschreibung in Ändern von Schutzzeitplänen).

Ändern der Cluster-Übertragungseinstellungen

In AppAssure können Sie die Einstellungen für die Verwaltung der Datenübertragung für einen geschützten Cluster ändern.

HINWEIS: Sie können Cluster-Übertragungseinstellungen nur ändern, wenn das Cluster freigegebene Volumes umfasst.

Es gibt drei verschieden Übertragungsarten in AppAssure:

- **Snapshots.** Sichert die Daten im geschützten Cluster.
- **VM Export.** Erstellt eine virtuelle Maschine mit allen Sicherungsinformationen und Parametern (gemäß Festlegung im Zeitplan für den Schutz des Clusters).
- **Wiederherstellen**. Stellt die gesicherten Informationen für einen geschützten Cluster wieder her.

So ändern Sie die Cluster-Übertragungseinstellungen

1. Navigieren Sie in der AppAssure Core Console zu dem Cluster, den Sie ändern möchten.
2. Klicken Sie auf die Registerkarte „Konfiguration“ und dann auf **Übertragungseinstellungen**.
3. Ändern Sie die Schutzeinstellungen (siehe Beschreibung in Ändern von Schutzzeitplänen).

Konvertieren eines geschützten Cluster-Knotens in einen Agenten

In AppAssure können Sie einen geschützten Cluster-Knoten in einen AppAssure Agent konvertieren, sodass dieser zwar weiterhin vom Core verwaltet wird, jedoch nicht mehr Bestandteil des Clusters ist. Dies ist beispielsweise nützlich, wenn Sie einen Cluster-Knoten aus dem Cluster entfernen müssen, der Knoten jedoch weiterhin geschützt sein soll.

So konvertieren Sie einen geschützten Cluster-Knoten in einen Agenten

1. Navigieren Sie in der AppAssure Core Console zu dem Cluster mit der Maschine, die konvertiert werden soll, und klicken Sie auf **Geschützte Knoten**.
2. Wählen Sie auf der Seite „Geschützte Knoten“ den gewünschten Knoten aus, und klicken Sie im Dropdown-Menü **Aktionen** auf **In Agent konvertieren**.

3 Um die Maschine wieder zum Cluster hinzuzufügen, wählen Sie die Maschine aus. Wählen Sie dann auf der Registerkarte **Zusammenfassung** im Menü „Aktionen“ die Option **In Cluster-Knoten konvertieren** aus, und klicken Sie dann auf **Ja**, um die Aktion zu bestätigen.

Anzeigen von Informationen für Server-Cluster

Führen Sie die folgenden Schritte aus, um Übersichts-, Ereignis-, Warninformationen usw. für Server-Cluster anzuzeigen.

Anzeigen von Cluster-Systeminformationen

Führen Sie die folgenden Schritte aus, um detaillierte Informationen für einen Cluster anzuzeigen.

So zeigen Sie Cluster-Systeminformationen an

1 Navigieren Sie in der AppAssure Core Console zu dem Cluster, den Sie anzeigen möchten.

2 Klicken Sie auf die Registerkarte „Extras“.

Die Seite mit Systeminformationen wird mit Systemdetails zum Cluster angezeigt, z. B. Name, enthaltene Knoten (jeweils mit Status und Windows-Version), Informationen zu Netzwerkschnittstellen sowie Informationen zur Volume-Kapazität.

Anzeigen von Cluster-Aufgaben, -Ereignissen und -Warnungen

Führen Sie die folgenden Schritte aus, um Ereignisse und Benachrichtigungen für einen Cluster anzuzeigen.

Weitere Informationen zum Anzeigen von Ereignissen und Benachrichtigungen für eine einzelne Maschine (Knoten) in einem Cluster finden Sie unter Anzeigen von Aufgaben, Benachrichtigungen und Ereignissen.

So zeigen Sie Cluster-Aufgaben, -Ereignisse und -Benachrichtigungen an

1 Navigieren Sie in der AppAssure Core Console zu dem Cluster, den Sie anzeigen möchten.

2 Klicken Sie auf die Registerkarte „Ereignisse“, um alle Aufgaben für den betreffenden Cluster anzuzeigen.

3 Sie können die Aufgaben filtern, die für den Cluster angezeigt werden. Weitere Informationen finden Sie unter Anzeigen von Aufgaben.

4 Um nur Benachrichtigungen anzuzeigen, klicken Sie oben links auf der Seite auf **Benachrichtigungen**.

Die Liste der Ereignisse wird so gefiltert, dass nur Benachrichtigungen des ausgewählten Clusters oder Knotens angezeigt werden.

5 Wenn Sie alle Benachrichtigungen auf der Seite löschen möchten, können Sie ggf. auf **Alle schließen** klicken.

6 Um alle Ereignisse anzuzeigen, klicken Sie oben links auf der Seite auf **Ereignisse**.

Für den ausgewählten Cluster oder Knoten werden alle Ereignisse angezeigt.

Anzeigen von zusammenfassenden Informationen

Führen Sie die folgenden Schritte aus, um zusammenfassende Informationen für einen Cluster anzuzeigen, z. B. Informationen zum Quorum für den Cluster.

So zeigen Sie zusammenfassende Informationen an

1. Navigieren Sie in der AppAssure Core Console zu dem Cluster, den Sie anzeigen möchten.
2. Auf der Registerkarte „Zusammenfassung“ werden Informationen wie Cluster-Name, Cluster-Typ, Quorumtyp (sofern zutreffend) und Quorumpfad (sofern zutreffend) angezeigt. Auf dieser Registerkarte werden auch Übersichtsinformationen zu den Volumes in diesem Cluster, z. B. Größe und Schutzzeitplan, angezeigt. Sofern zutreffend können auch SQL Server- oder Exchange Server-Informationen für einen anderen Cluster angezeigt werden.
3. Um die Informationen zu aktualisieren, klicken Sie im Dropdown-Menü **Aktionen** auf **Metadaten aktualisieren**.

Weitere Informationen zum Anzeigen von Übersichts- und Statusinformationen für eine einzelne Maschine (Knoten) in einem Cluster finden Sie unter Anzeigen des Maschinenstatus und anderen Details.

Verwenden von Cluster-Wiederherstellungspunkten

Ein Wiederherstellungspunkt – auch als Snapshot bezeichnet – ist eine Kopie der Ordner und Dateien für die freigegebenen Volumes in einem Cluster, die im Repository gespeichert sind, zu einem bestimmten Zeitpunkt. Wiederherstellungspunkte werden für die Wiederherstellung geschützter Maschinen oder für die Bereitstellung in einem lokalen Dateisystem verwendet. In AppAssure können Sie eine Liste der Wiederherstellungspunkte im Repository anzeigen. Führen Sie die folgenden Schritte aus, um Wiederherstellungspunkte zu überprüfen.

HINWEIS: Wenn Sie Daten eines DAG- oder CCR-Server-Clusters schützen, werden die zugehörigen Wiederherstellungspunkte nicht auf Cluster-Ebene angezeigt. Sie sind nur auf Knoten- oder Maschinenebene sichtbar.

Informationen zum Anzeigen von Wiederherstellungspunkten für einzelne Maschinen in einem Cluster finden Sie unter Anzeigen von Wiederherstellungspunkten.

So arbeiten Sie mit Cluster-Wiederherstellungspunkten

1. Navigieren Sie in der AppAssure Core Console zu dem Cluster, für den Sie Wiederherstellungspunkte anzeigen möchten.
2. Klicken Sie auf die Registerkarte „Wiederherstellungspunkte“.
3. Klicken Sie zum Anzeigen ausführlicher Informationen zu einem bestimmten Wiederherstellungspunkt auf das Symbol der rechten spitzen Klammer > neben einem Wiederherstellungspunkt in der Liste, um die Ansicht zu erweitern.
4. Weitere Informationen zu den Vorgängen, die Sie für Wiederherstellungspunkte durchführen können, finden Sie unter Anzeigen eines bestimmten Wiederherstellungspunkts.
5. Wählen Sie einen Wiederherstellungspunkt aus, der bereitgestellt werden soll.

   Informationen zum Bereitstellen eines Wiederherstellungspunkts finden Sie unter Bereitstellen eines Wiederherstellungspunktes für eine Windows-Maschine.
6. Informationen zum Löschen von Wiederherstellungspunkten finden Sie unter Entfernen von Wiederherstellungspunkten.

Verwalten von Snapshots für einen Cluster

In AppAssure können Sie Snapshots verwalten, indem Sie das Erstellen eines Snapshots erzwingen oder die Snapshot-Erstellung vorübergehend deaktivieren. Durch das Erzwingen der Snapshot-Erstellung können Sie eine Datenübertragung für die aktuelle geschützte Maschine erzwingen. Wenn Sie eine Snapshot-Erstellung erzwingen, wird die Übertragung entweder sofort gestartet oder zur Warteschlange hinzugefügt. Dabei werden nur die Daten übertragen, die seit einem vorherigen Wiederherstellungspunkt geändert wurden. Falls kein vorheriger Wiederherstellungspunkt vorhanden ist, werden alle Daten (das Basisimage) auf den geschützten Volumes übertragen. Wenn Sie die Snapshot-Erstellung vorübergehend deaktivieren, werden vorübergehend alle Übertragungen der Daten von der aktuellen Maschine angehalten.

Informationen zum Erzwingen von Snapshots für die einzelnen Maschinen im Cluster finden Sie unter Erzwingen eines Snapshots. Informationen zum vorübergehenden Deaktivieren und erneuten Aktivieren der Snapshot-Erstellung für die einzelnen Maschinen im Cluster finden Sie unter Vorübergehendes Deaktivieren und erneutes Aktivieren der Schutzfunktion.

Erzwingen der Snapshot-Erstellung für einen Cluster

Führen Sie die folgenden Schritte aus, um die Snapshot-Erstellung für einen Cluster zu erzwingen.

So erzwingen Sie die Snapshot-Erstellung für einen Cluster

1. Navigieren Sie in der AppAssure Core Console zu dem Cluster, für den Sie Wiederherstellungspunkte anzeigen möchten.
2. Klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü **Aktionen** auf **Snapshot erzwingen**.

Anhalten und Fortsetzen der Erstellung von Cluster-Snapshots

Führen Sie die folgenden Schritte aus, um die Snapshot-Erstellung für einen Cluster anzuhalten und wieder fortzusetzen.

So deaktivieren Sie die Snapshot-Erstellung vorübergehend und aktivieren Sie die Snapshot-Erstellung wieder

1. Navigieren Sie in der AppAssure Core Console zu dem Cluster, für den Sie Wiederherstellungspunkte anzeigen möchten.
2. Klicken Sie auf der Registerkarte „Zusammenfassung“ im Dropdown-Menü **Aktionen** auf **Schutz vorübergehend deaktivieren**.
3. Wählen Sie im Dialogfeld „Schutz vorübergehend deaktivieren“ eine der in der folgenden Tabelle beschriebenen Optionen aus.

Tabelle 99.

Option	Beschreibung
Deaktivieren bis Wiederaktivierung	Die Snapshot-Erstellung wird vorübergehend deaktiviert, bis der Schutz wieder manuell aktiviert wird. • Klicken Sie im Menü **Aktionen** auf **Wieder aktivieren**, um den Schutz wieder zu aktivieren
Vorübergehend deaktivieren für (Dauer)	Hier können Sie einen Zeitraum in Tagen, Stunden und Minuten angeben, für den die Snapshot-Erstellung vorübergehend deaktiviert werden soll.

Aufheben der Bereitstellung lokaler Wiederherstellungspunkte

Führen Sie die folgenden Schritte aus, um die Bereitstellung von Wiederherstellungspunkten aufzuheben, die lokal bereitgestellt wurden.

So heben Sie die Bereitstellung lokaler Wiederherstellungspunkte auf

1. Navigieren Sie in der AppAssure Core Console zu dem Cluster, für den Sie die Bereitstellung von Wiederherstellungspunkten aufheben möchten.
2. Klicken Sie auf der Registerkarte „Extras“ im Menü „Extras“ auf **Bereitstellungen**.
3. Führen Sie in der Liste der lokalen Bereitstellungen eine der folgenden Aktionen aus:
   - Um eine einzelne lokale Bereitstellung aufzuheben, wählen Sie die Bereitstellung für den Wiederherstellungspunkt aus, die Sie entfernen möchten, und klicken Sie dann auf **Bereitstellung aufheben**.
   - Klicken Sie auf die Schaltfläche **Alle Bereitstellungen aufheben**, um alle lokalen Bereitstellungen aufzuheben.

Durchführen einer Wiederherstellung für Cluster und Cluster-Knoten

Bei einer Wiederherstellung werden die Volumes auf einer Maschine aus Wiederherstellungspunkten wiederhergestellt. Bei einem Server-Cluster wird die Wiederherstellung auf Knoten- oder Maschinenebene durchgeführt. Dieser Abschnitt enthält Richtlinien zum Durchführen einer Wiederherstellung für Cluster-Volumes.

Durchführen einer Wiederherstellung für CCR- (Exchange) und DAG-Cluster

Führen Sie die folgenden Schritte aus, um eine Wiederherstellung für CCR- (Exchange) und DAG-Cluster durchzuführen.

So führen Sie eine Wiederherstellung für CCR- (Exchange) und DAG-Cluster durch

1. Schalten Sie alle Knoten bis auf einen aus.
2. Führen Sie eine Wiederherstellung mit dem Standardverfahrens von AppAssure für die Maschine durch (siehe Beschreibung in Wiederherstellen von Volumes aus einem Wiederherstellungspunkt und Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile).
3. Stellen Sie nach der Wiederherstellung Sie alle Datenbanken für die Cluster-Volumes bereit.
4. Schalten Sie alle anderen Knoten ein.
5. Navigieren Sie bei Exchange zur Exchange-Verwaltungskonsole und führen Sie für jede Datenbank den Vorgang **Datenbankkopie aktualisieren** aus.

Durchführen einer Wiederherstellung für SCC-Cluster (Exchange, SQL)

Führen Sie die folgenden Schritte aus, um eine Wiederherstellung für CCR-Cluster (Exchange, SQL) durchzuführen.

So führen Sie eine Wiederherstellung für SCC-Cluster (Exchange, SQL) durch

1. Schalten Sie alle Knoten bis auf einen aus.
2. Führen Sie eine Wiederherstellung mit dem Standardverfahrens von AppAssure für die Maschine durch (siehe Beschreibung in Wiederherstellen von Volumes aus einem Wiederherstellungspunkt und Wiederherstellen von Volumes einer Linux-Maschine über die Befehlszeile).
3. Stellen Sie nach der Wiederherstellung Sie alle Datenbanken der Cluster-Volumes bereit.
4. Schalten Sie alle anderen Knoten einzeln nacheinander ein.

> **HINWEIS:** Sie brauchen kein Rollback für den Quorumdatenträger durchzuführen. Er kann automatisch oder mithilfe der Cluster-Dienstfunktionalität neu erstellt werden.

Replizieren von Cluster-Daten

Wenn Sie Daten für einen Cluster replizieren, müssen Sie den gesamten Cluster replizieren. Wenn Sie beispielsweise einen Knoten auswählen, der replizier werden soll, wird automatisch der Cluster ausgewählt. Wenn Sie den Cluster auswählen, werden ebenso alle Knoten im Cluster ausgewählt.

Weitere Informationen und Anweisungen zum Replizieren von Daten finden Sie unter Anleitung für die Einrichtung der Replikation.

Aufheben des Clusters-Schutzes

Führen Sie die folgenden Schritte aus, um den Schutz eines Cluster aufzuheben.

So heben Sie den Cluster-Schutz auf

1. Navigieren Sie in der AppAssure Core Console zu dem Cluster, den Sie entfernen möchten.
2. Klicken Sie im Dropdown-Menü **Aktionen** auf **Maschine entfernen**.
3. Wählen Sie eine der folgenden Optionen aus.

Tabelle 100.

Option	Beschreibung
Wiederherstellungspunkte beibehalten	Um alle derzeit gespeicherten Wiederherstellungspunkte für diesen Cluster beizubehalten.
Wiederherstellungspunkte entfernen	Um alle derzeit gespeicherten Wiederherstellungspunkte für diesen Cluster aus dem Repository zu entfernen.

Aufheben des Schutzes von Cluster-Knoten

Führen Sie die folgenden Schritte aus, um den Schutz eines Cluster aufzuheben.

Informationen zum Entfernen eines einzigen Knotens aus dem Cluster finden Sie unter Konvertieren eines geschützten Cluster-Knotens in einen Agenten.

So heben Sie den Schutz eines Cluster-Knoten auf

1. Navigieren Sie in der AppAssure Core Console zur Registerkarte „Geschützte Knoten“ des Clusters.
2. Klicken Sie im Dropdown-Menü „Aktionen“ auf **Maschine entfernen**.
3. Wählen Sie eine der in der folgenden Tabelle beschriebenen Optionen aus.

Tabelle 101.

Option	Beschreibung
Wiederherstellungspunkte beibehalten	Um alle derzeit gespeicherten Wiederherstellungspunkte für diese Maschine oder diesen Knoten beizubehalten.
Wiederherstellungspunkte entfernen	Um alle derzeit gespeicherten Wiederherstellungspunkte für diese Maschine oder diesen Knoten aus dem Repository zu entfernen.

Aufheben des Schutzes aller Knoten in einem Cluster

Führen Sie die folgenden Schritte aus, um den Schutz aller Knoten in einem Cluster aufzuheben.

△ | **VORSICHT: Wenn Sie alle Cluster-Knoten entfernen, wird auch der Cluster entfernt.**

So heben Sie den Schutz aller Knoten in einem Cluster auf

1. Navigieren Sie in der AppAssure Core Console zur Registerkarte „Geschützte Knoten“ des Clusters.
2. Wählen Sie auf der Registerkarte „Geschützte Knoten“ alle Knoten aus.
3. Klicken Sie im Dropdown-Menü „Aktionen“ oben in der Registerkarte „Geschützte Knoten“ auf **Alle Knoten entfernen**, und wählen Sie dann eine der in der folgenden Tabelle beschriebenen Optionen aus.

Tabelle 102.

Option	Beschreibung
Wiederherstellungspunkte beibehalten	Um alle derzeit gespeicherten Wiederherstellungspunkte für diesen Cluster beizubehalten.
Wiederherstellungspunkte entfernen	Um alle derzeit gespeicherten Wiederherstellungspunkte für diesen Cluster aus dem Repository zu entfernen.

Anzeigen eines Cluster- oder Knotenberichts

Sie können Compliance- und Fehlerberichte zu AppAssure-Aktivitäten für den Cluster und einzelne Knoten anzeigen. Die Berichte enthalten Informationen zu AppAssure-Aktivitäten für Cluster, Knoten und freigegebene Volumes.

Weitere Informationen zu AppAssure-Berichten finden Sie unter Informationen zu Berichten. Weitere Informationen zu den Druck- und Exportoptionen in der Symbolleiste für Berichte finden Sie unter Informationen zur Symbolleiste für Berichte.

So zeigen Sie einen Cluster- oder Knotenbericht an

1 Navigieren Sie in der AppAssure Core Console zu dem Cluster, für den Sie einen Bericht erstellen möchten.

2 Wählen Sie einen Knoten aus, wenn Sie einen Bericht für einen Knoten in einem Cluster erstellen möchten.

3 Klicken Sie auf die Registerkarte „Extras“ und wählen Sie im Menü „Berichte“ eine der folgenden Optionen aus:

- Compliancebericht
- Fehlerbericht

4 Wählen Sie im Dropdown-Kalender „Start Time“ ein Startdatum aus, und geben Sie dann eine Startzeit für den Bericht ein.

> **HINWEIS:** Daten stehen erst zur Verfügung, nachdem der AppAssure Core bzw. Agent bereitgestellt wurde.

5 Wählen Sie im Dropdown-Kalender „End Time“ ein Enddatum aus, und geben Sie dann eine Endzeit für den Bericht ein.

6 Klicken Sie auf **Bericht generieren**. Die Ergebnisse des Berichts werden auf der Seite angezeigt.

Wenn der Bericht mehrere Seiten umfasst, können Sie auf die Seitenzahlen oder auf die Pfeilschaltflächen am Anfang der Berichtsergebnisse klicken, um durch die Ergebnisse zu navigieren.

7 Wählen Sie das gewünschte Exportformat in der Dropdown-Liste, um die Berichtsergebnisse in eines der verfügbaren Formate (PDF, XLS, XLSX, RTF, MHT, HTML, TXT, CSV oder Bilddatei) zu exportieren, und führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf das erste Speichersymbol, um einen Bericht zu exportieren und auf dem Datenträger zu speichern.
- Klicken Sie auf das zweite Speichersymbol, um einen Bericht zu exportieren und in einem neuen Webbrowserfenster anzuzeigen.

8 Führen Sie zum Drucken der Berichtsergebnisse einen der folgenden Schritte aus:

- Klicken Sie auf das erste Druckersymbol, um den gesamten Bericht zu drucken.
- Klicken Sie auf das zweite Druckersymbol, um die aktuelle Seite des Berichts zu drucken.

5

Berichterstellung

Dieses Kapitel bietet einen Überblick über die Berichterstellungsfunktionen in Dell AppAssure. Folgende Themen werden behandelt:

- Informationen zu Berichten
- Informationen zu Complianceberichten
- Informationen zu Fehlerberichten
- Informationen zu Zusammenfassungsberichten
- Erstellen eines Berichts für einen Core oder Agenten
- Informationen zu Berichten für Cores in der Central Management Console
- Erstellen eines Berichts in der Central Management Console

Informationen zu Berichten

Sie können in AppAssure Compliance-, Fehler- und Übersichtsinformationen für mehrere Core- und Agent-Maschinen erstellen und anzeigen.

Sie können Berichte online anzeigen, Berichte drucken oder exportieren und in mehreren unterstützten Formaten speichern. Die folgenden Formate sind verfügbar:

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- Bild

In diesem Release von AppAssure enthalten die Berichte jetzt Maßeinheiten, damit Sie leichter feststellen können, ob eine Spalte in GB, TB oder in Sekunden dargestellt wird.

Informationen zur Symbolleiste für Berichte

Die für alle Berichte verfügbare Symbolleiste bietet zwei Möglichkeiten, Berichte zu drucken und zu speichern. Die Druck- und Speicheroptionen sind in der folgenden Tabelle beschrieben.

Tabelle 103.

Symbol	Beschreibung
	Bericht drucken
	Aktuelle Seite drucken
	Bericht exportieren und auf dem Datenträger speichern

Informationen zum Erstellen von Berichten finden Sie unter Erstellen eines Berichts für einen Core oder Agenten. Informationen zum Erstellen von Berichten für mehrere Cores in der Central Management Console finden Sie unter Erstellen eines Berichts in der Central Management Console. Informationen zum Erstellen von Berichten für Cluster finden Sie unter Anzeigen eines Cluster- oder Knotenberichts.

Informationen zu Complianceberichten

Complianceberichte sind für den AppAssure Core und für den AppAssure Agent verfügbar. Sie können damit den Status von Jobs anzeigen, die von einem bestimmten Core oder Agenten durchgeführt wurden. Fehlgeschlagene Jobs werden rot angezeigt. Informationen im Core-Compliancebericht, die keinem Agenten zugewiesen sind, bleiben leer.

Die Details zu den Jobs werden in einer Spaltenansicht angezeigt, die die folgenden Kategorien umfasst:

- Core
- Geschützter Agent
- Typ
- Zusammenfassung
- Status
- Fehler
- Startzeit
- Endzeit
- Uhrzeit
- Arbeit, gesamt

Informationen zum Erstellen von Berichten finden Sie unter Erstellen eines Berichts für einen Core oder Agenten.

Informationen zu Fehlerberichten

Fehlerberichte enthalten eine Teilmenge der Informationen im Compliancebericht und sind für AppAssure Cores sowie AppAssure Agents verfügbar. Fehlerberichte enthalten nur die fehlgeschlagenen Jobs, die im Compliancebericht aufgeführt sind. Sie werden in einem einzelnen Bericht zusammengefasst und können gedruckt sowie exportiert werden.

Die Details zu den Fehlern werden in einer Spaltenansicht mit den folgenden Kategorien angezeigt:

- Core
- Agent
- Typ
- Zusammenfassung
- Fehler
- Startzeit
- Endzeit
- Abgelaufene Zeit
- Arbeit, gesamt

Informationen zum Erstellen von Berichten finden Sie unter Erstellen eines Berichts für einen Core oder Agenten.

Informationen zu Zusammenfassungsberichten

Der Zusammenfassungsbericht enthält Informationen zu den Repositorys des ausgewählten AppAssure Core sowie zu den durch den Core geschützten Agenten. Die Informationen werden in zwei Übersichten in einem Bericht angezeigt. Informationen zum Erstellen von Zusammenfassungsberichten finden Sie unter Erstellen eines Berichts für einen Core oder Agenten.

Repositoryübersicht

Der Repositoryabschnitt des Zusammenfassungsberichts enthält Daten zu den Repositorys, die sich im ausgewählten AppAssure Core befinden. Die Details zu den Repositorys werden in einer Spaltenansicht mit den folgenden Kategorien angezeigt:

- Name
- Datenpfad
- Metadatenpfad
- Zugewiesener Speicherplatz
- Verwendeter Speicherplatz
- Freier Speicherplatz
- Komprimierungs-/Deduplizierungsverhältnis

HINWEIS: Zugewiesener, verwendeter und freier Speicherplatz werden mit der entsprechenden Maßeinheit angezeigt. Als Maßeinheiten werden GB, TB oder Sekunden verwendet.

Agentenübersicht

Der Agentenabschnitt des Zusammenfassungsberichts enthält Daten zu den Agenten, die durch den ausgewählten AppAssure Core geschützt werden.

Die Details zu den Agenten werden in einer Spaltenansicht mit den folgenden Kategorien angezeigt:

- Name
- Geschützte Volumes
- Geschützter Speicherplatz, gesamt
- Derzeit geschützter Speicherplatz
- Änderungsrate pro Tag (Durchschnitt | Median)
- Jobstatistik (Erfolgreich | Fehlgeschlagen | Abgebrochen)

Erstellen eines Berichts für einen Core oder Agenten

Führen Sie die folgenden Schritte aus, um einen Bericht für einen AppAssure Core oder AppAssure Agent zu erstellen.

So erstellen Sie einen Bericht für einen Core oder Agenten

1 Navigieren Sie zur AppAssure Core Console, und wählen Sie den Core oder den Agenten aus, für den der Bericht erstellt werden soll.

2 Klicken Sie auf die Registerkarte „Extras“.

3 Erweitern Sie auf der Registerkarte „Extras“ im linken Navigationsbereich **Berichte**.

4 Wählen Sie im linken Navigationsbereich den Bericht aus, den Sie erstellen möchten. Die jeweils verfügbaren Berichte hängen von der in Schritt 1 vorgenommenen Auswahl ab. Eine Beschreibung der Berichte finden Sie in der folgenden Tabelle.

Tabelle 104.

Maschine	Verfügbare Berichte
Core	Compliancebericht
	Zusammenfassender Bericht
	Fehlerbericht
Agent	Compliancebericht
	Fehlerbericht

5 Wählen Sie im Dropdown-Kalender „Start Time“ ein Startdatum aus, und geben Sie dann eine Startzeit für den Bericht ein.

HINWEIS: Daten stehen erst zur Verfügung, nachdem der Core bzw. der Agent bereitgestellt wurde.

6 Wählen Sie im Dropdown-Kalender „End Time“ ein Enddatum aus, und geben Sie dann eine Endzeit für den Bericht ein.

7 Aktivieren Sie für einen Zusammenfassungsbericht das Kontrollkästchen **Alle Zeiten**, wenn Startzeit und Endzeit die Nutzungszeit des Core abdecken sollen.

8 Wählen Sie bei einem Compliance- oder Fehlerbericht in der Dropdown-Liste für die Ziel-Cores den Core aus, für den die Daten angezeigt werden sollen.

9 Klicken Sie auf **Bericht generieren**.

Nachdem der Bericht erstellt wurde, können Sie den Bericht über die Symbolleiste drucken oder exportieren. Weitere Informationen zur Symbolleiste finden Sie unter Informationen zur Symbolleiste für Berichte.

Informationen zu Berichten für Cores in der Central Management Console

Sie können in AppAssure Compliance-, Fehler- und Übersichtsinformationen für mehrere AppAssure Cores erstellen und anzeigen. Die Details zu den Core werden in einer Spaltenansicht mit den in den Abschnitten Informationen zu Complianceberichten, Informationen zu Fehlerberichten und Informationen zu Zusammenfassungsberichten aufgeführten Kategorien angezeigt.

Informationen zum Erstellen von Berichten für mehrere Cores finden Sie unter Erstellen eines Berichts in der Central Management Console.

Erstellen eines Berichts in der Central Management Console

Führen Sie die folgenden Schritte aus, um in der Central Management Console einen Bericht für mehrere AppAssure Cores zu erstellen.

So erstellen Sie einen Bericht in der Central Management Console

1. Klicken Sie auf der Begrüßungsseite der Central Management Console auf das Dropdown-Menü in der oberen rechten Ecke.
2. Klicken Sie im Dropdown-Menü auf **Berichte** und wählen Sie dann eine der folgenden Optionen aus:
   - Compliancebericht
   - Zusammenfassender Bericht
   - Fehlerbericht
3. Wählen Sie im linken Navigationsbereich die AppAssure Cores aus, für die Sie den Bericht erstellen möchten.
4. Wählen Sie im Dropdown-Kalender „Start Time“ ein Startdatum aus, und geben Sie dann eine Startzeit für den Bericht ein.

   HINWEIS: Daten sind erst dann verfügbar, nachdem die Cores bereitgestellt wurden.

5. Wählen Sie im Dropdown-Kalender „End Time“ ein Enddatum aus, und geben Sie dann eine Endzeit für den Bericht ein.
6. Klicken Sie auf **Bericht generieren**.

   Nachdem der Bericht erstellt wurde, können Sie den Bericht über die Symbolleiste drucken oder exportieren. Weitere Informationen zur Symbolleiste finden Sie unter Informationen zur Symbolleiste für Berichte.

A

Skripterstellung

AppAssure bietet Administratoren die Möglichkeit, die Administration und Verwaltung von Ressourcen in bestimmten Situationen durch Ausführung von Befehlen und Skripts zu automatisieren. Die AppAssure-Software unterstützt die Erstellung von PowerShell-Skripts für Windows und Bourne Shell-Skripts für Linux.

△ **VORSICHT: Die in diesem Dokument enthaltenen PowerShell- und Bourne-Beispielskripts funktionieren, wenn Sie in der vorliegenden Form von qualifizierten Administratoren ausgeführt werden. Achten Sie beim Ändern funktionierender Skripts darauf, dass Sie funktionsfähige Versionen behalten. Jedwede Änderungen der hier enthaltenen Skriptbeispiele oder alle selbst erstellten benutzerdefinierten Skripts werden als Anpassungen angesehen, die normalerweise nicht vom Kunden-Support abgedeckt werden.**

In diesem Anhang werden sie Skripts beschrieben, die Administratoren in den jeweiligen Situationen in AppAssure für Windows und Linux verwenden können. Folgende Themen werden behandelt:

- PowerShell Scripting in AppAssure
- Eingabeparameter für PowerShell-Skripts
- Beispiele für PowerShell-Skripts
- Informationen zum Erstellen von Bourne Shell-Skripts in AppAssure
- Eingabeparameter für Bourne Shell-Skripts
- Beispiele für Bourne Shell-Skripts

PowerShell Scripting in AppAssure

Windows PowerShell ist eine an Microsoft .NET Framework gebundene Umgebung für die Verwaltungsautomatisierung. AppAssure enthält umfassende SDKs für die Erstellung von PowerShell-Skripts, mit denen Administratoren in bestimmten Situationen benutzerdefinierte PowerShell-Skripts ausführen können, z. B. vor oder nach der Snapshot-Erstellung, vor oder nach Anfügbarkeits- und Bereitstellbarkeitsprüfungen usw. Administratoren können Skripts auf dem AppAssure Core als auch auf Agenten ausführen. Skripts können Parameter übernehmen. Die Ausgabe eines Skripts wird in die Protokolldateien des Core oder Agenten geschrieben.

ⓘ **HINWEIS:** Bei nächtlichen Jobs sollten Sie jeweils eine Skriptdatei und den Eingabeparameter *JobType* speichern, um die nächtlichen Jobs unterscheiden zu können.

Skriptdateien befinden sich im Ordner %ALLUSERSPROFILE%\AppRecovery\Scripts.

- In Windows 7 lautet der Pfad zum Order %ALLUSERSPROFILE%: C:\ProgramData.
- In Windows 2003 lautet der Pfad zum Order: Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\.

ⓘ **HINWEIS:** Windows PowerShell ist erforderlich und muss installiert und konfiguriert werden, damit AppAssure-Skripts verwendet und ausgeführt werden können.

Weitere Informationen zur Verwendung von PowerShell-Skripts finden Sie unter Beispiele für PowerShell-Skripts, Eingabeparameter für PowerShell-Skripts und Beispiele für Bourne Shell-Skripts.

Voraussetzungen für die Erstellung von PowerShell-Skripts

Damit Sie die PowerShell-Skripts für AppAssure verwenden und ausführen können, muss Windows PowerShell 3.0 installiert sein.

HINWEIS: Die Datei „powershell.exe.config“ muss sich im Basisverzeichnis von PowerShell befinden, z. B. C:\WindowsPowerShell\powershell.exe.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
      <startup useLegacyV2RuntimeActivationPolicy="true">
            <supportedRuntime version="v4.0.30319"/>
            <supportedRuntime version="v2.0.50727"/>
      </startup>
</configuration>
```

Testen von PowerShell-Skripts

Mit dem grafischen Editor von PowerShell *powershell_is* können Sie die Skripts, die Sie ausführen möchten, testen. Sie müssen die Konfigurationsdatei *powershell_ise.exe.config* zum selben Ordner hinzufügen, in dem sich die Konfigurationsdatei *powershell.exe.config* befindet.

HINWEIS: Die Konfigurationsdatei *powershell_ise.exe.config* muss den gleichen Inhalt wie die Datei *powershell.exe.config* haben.

VORSICHT: Wenn das PowerShell-Vor- oder Nachskript fehlschlägt, schlägt auch der Job fehl.

Eingabeparameter für PowerShell-Skripts

In den Beispielskripts werden alle verfügbaren Eingabeparameter verwendet. Die Parameter werden in den folgenden Tabellen beschrieben.

HINWEIS: Die Skriptdateien müssen den gleichen Namen wie die Beispielskriptdateien aufweisen.

AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents)

Die folgende Tabelle enthält die verfügbaren Objekte für den AgentProtectionStorageConfiguration-Parameter.

Tabelle 105.

Methode	Beschreibung
public Guid RepositoryId { get; set; }	Ruft die ID des Repositorys, in dem die Wiederherstellungspunkte der Agenten gespeichert sind, ab oder legt diese fest.
public string EncryptionKeyId { get; set; }	Ruft die ID des Verschlüsselungsschlüssels für die Wiederherstellungspunkte des betreffenden Agenten ab oder legt diese fest. Eine leere Zeichenfolge bedeutet keine Verschlüsselung.

AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

Die folgende Tabelle enthält die verfügbaren Objekte für den AgentTransferConfiguration-Parameter.

Tabelle 106.

Methode	Beschreibung
public uint MaxConcurrentStreams { get; set; }	Ruft die maximale Anzahl gleichzeitiger TCP-Verbindungen, die der Core für die Datenübertragung zum Agenten herstellt, ab oder legt diese fest.
public uint MaxTransferQueueDepth { get; set; }	Wird ein Blockbereich aus einem Übertragungsstream gelesen, wird dieser Bereich in eine Producer-/Consumer-Warteschlange eingereiht und dort von einem Consumer-Thread gelesen und in das Epoch-Objekt geschrieben. Wenn das Repository langsamer schreibt als das Netzwerk liest, füllt sich die Warteschlange. Der Punkt, an dem die Warteschlange voll ist und der Lesevorgang stoppt, wird als maximale Tiefe der Übertragungswarteschlange bezeichnet.
public uint MaxConcurrentWrites { get; set; }	Ruft die maximale Anzahl der Blockschreibvorgänge, die zu einem bestimmten Zeitpunkt für eine Epoche ausstehen, ab oder legt diese fest. Werden weitere Blöcke empfangen, während noch so viele Blockschreibvorgänge ausstehen, werden diese zusätzlichen Blöcke ignoriert, bis einer der ausstehenden Schreibvorgänge beendet wurde.
public ulong MaxSegmentSize { get; set; }	Ruft die maximale Anzahl zusammenhängender Blöcke für die Übertragung einer einzelnen Anforderung ab oder legt diese fest. Abhängig vom jeweiligen Test sind höhere oder niedrigere Werte besser geeignet.
public Priority Priority { get; set; }	Ruft die Priorität von Übertragungsanforderungen ab oder legt diese fest.
public int MaxRetries { get; set; }	Ruft die maximale Anzahl von Wiederholungsversuchen bei einer fehlerhaften Übertragung ab oder legt diese fest, bis die Übertragung als fehlgeschlagen angesehen wird.
public Guid ProviderId{ get; set; }	Ruft die GUID des VSS-Anbieters ab oder legt diese fest, der für Snapshots auf diesem Host verwendet werden soll. Administratoren übernehmen normalerweise die Standardeinstellung.
public Collection<ExcludedWriter> ExcludedWriterIds { get; set; }	Ruft die VSS-Writer-IDs, die aus diesem Snapshot ausgeschlossen werden sollen, ab oder legt diese fest. Die Writer-ID wird durch den Namen des Writers bestimmt. Dieser Name dient lediglich zu Dokumentationszwecken und muss nicht exakt mit dem Namen des Writers übereinstimmen.

Tabelle 106.

Methode	Beschreibung
public ushort TransferDataServerPort { get; set; }	Ruft einen Wert ab oder legt diesen fest, in dem der TCP-Port enthalten ist, über den Verbindungen vom Core für die eigentliche Datenübertragung vom Agenten zum Core hergestellt werden. Der Agent versucht, über den Port zu kommunizieren. Wenn der Port jedoch verwendet wird, kann der Agent auch einen anderen Port verwenden. Der Core sollte die Portnummer verwenden, die in den Eigenschaften „BlockHashesUri“ und „BlockDataUri“ des Objekts „VolumeSnapshotInfo“ für die einzelnen Volume angegeben ist, für die ein Snapshot erstellt wurde.
public TimeSpan SnapshotTimeout { get; set; }	Ruft den Zeitraum ab oder legt diesen fest, für den auf den Abschluss einer VSS-Snapshot-Erstellung gewartet wird, bevor der Vorgang wegen Zeitüberschreitung abgebrochen wird.
public TimeSpan TransferTimeout { get; set; }	Ruft den Zeitraum ab oder legt diesen fest, für den auf einen weiteren Core-Kontakt gewartet wird, bevor die Snapshot-Erstellung abgebrochen wird.
public TimeSpan NetworkReadTimeout { get; set; }	Ruft das Zeitlimit für Netzwerklesevorgänge der jeweiligen Übertragung ab oder legt dieses fest.
public TimeSpan NetworkWriteTimeout { get; set; }	Ruft das Zeitlimit für Netzwerkschreibvorgänge der jeweiligen Übertragung ab oder legt dieses fest.

BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

Die folgende Tabelle enthält die verfügbaren Objekte für den BackgroundJobRequest-Parameter.

Tabelle 107.

Methode	Beschreibung
public Guid AgentId { get; set; }	Ruft die Agenten-ID ab oder legt diese fest.
public bool IsNightlyJob { get; set; }	Ruft den Wert, der angibt, ob der Hintergrundjob ein nächtlicher Job ist, ab oder legt diesen fest.
public virtual bool InvolvesAgentId(Guid agentId)	Ermittelt den Wert, der angibt, ob der jeweilige Agent am Job beteiligt ist.

ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

Übernimmt die jeweiligen Werte vom DatabaseCheckJobRequestBase-Parameter.

DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)

Übernimmt die jeweiligen Werte vom BackgroundJobRequest-Parameter.

ExportJobRequest (namespace Replay.Core.Contracts.Export)

Übernimmt die jeweiligen Werte vom BackgroundJobRequest-Parameter.

Die folgende Tabelle enthält die verfügbaren Objekte für den ExportJobRequest-Parameter.

Tabelle 108.

Methode	Beschreibung
public uint RamInMegabytes { get; set; }	Ruft die Hauptspeichergröße für die exportierte VM ab oder legt diese fest. Legen Sie diesen Wert auf null (0) fest, wenn die Speichergröße der Quellmaschine verwendet werden soll.
public VirtualMachineLocation Location { get; set; }	Ruft den Zielspeicherorts für diesen Export ab oder legt diesen fest. Hierbei handelt es sich um eine abstrakte Basisklasse.
public VolumeImageIdsCollection VolumeImageIds { get; private set; }	Ruft die Volume-Images ab oder legt diese fest, die im VM-Export enthalten sein sollen.
public ExportJobPriority Priority { get; set; }	Ruft die Priorität von Exportanforderungen ab oder legt diese fest.

NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql)

Übernimmt die jeweiligen Werte vom BackgroundJobRequest-Parameter.

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

Übernimmt die jeweiligen Werte vom BackgroundJobRequest-Parameter.

TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)

Die folgende Tabelle enthält die verfügbaren Objekte für den TakeSnapshotResponse-Parameter.

Tabelle 109.

Methode	Beschreibung
public Guid SnapshotSetId { get; set; }	Ruft die GUID ab oder legt diese fest, die diesem Snapshot von VSS zugewiesen wurde.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Ruft die Snapshot-Informationen für jedes Volume, das im Snapshot enthalten ist, ab oder legt diese fest.

TransferJobRequest (namespace Replay.Core.Contracts.Transfer)

Übernimmt die jeweiligen Werte vom BackgroundJobRequest-Parameter.

Die folgende Tabelle enthält die verfügbaren Objekte für den TransferJobRequest-Parameter.

Tabelle 110.

Methode	Beschreibung
public VolumeNameCollection VolumeNames { get; set; }	Ruft die Namen für die Übertragung ab oder legt diese fest. VolumeNames ist eine Datenstruktur, die die folgenden Daten enthält: • GuidName - Die dem Volume zugeordnete GUID, die als Name verwendet wird, wenn DisplayName nicht festgelegt ist. • DisplayName - Der Anzeigename des Volumes.
public ShadowCopyType ShadowCopyType { get; set; }	Ruft die Art des Kopiervorgangs für die Übertragung ab oder legt diese fest. Die folgenden Werte sind verfügbar: • Unknown • Copy • Full
public AgentTransferConfiguration TransferConfiguration { get; set; }	Ruft die Übertragungskonfiguration ab oder legt diese fest.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Ruft die Speicherkonfiguration ab oder legt diese fest.
public string Key { get; set; }	Erzeugt einen pseudozufälligen (aber kryptografisch nicht sicheren) Schlüssel, der als einmaliges Kennwort für die Authentifizierung von Übertragungsanforderungen verwendet werden kann.
public bool ForceBaseImage { get; set; }	Ruft den Wert, der angibt, ob das Basisimage erzwungen wurde oder nicht, ab oder legt diesen fest.
public bool IsLogTruncation { get; set; }	Ruft den Wert, der angibt, ob das Protokoll des Jobs gekürzt wurde oder nicht, ab oder legt diesen fest.

TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Die folgende Tabelle enthält die verfügbaren Objekte für den TransferPrescript-Parameter.

Tabelle 111.

Methode	Beschreibung
public VolumeNameCollection VolumeNames (get; set;)	Ruft die Volume-Namen für die Übertragung ab oder legt diese fest. VolumeNames ist eine Datenstruktur, die die folgenden Daten enthält: • GuidName - Die dem Volume zugeordnete GUID, die als Name verwendet wird, wenn DisplayName nicht festgelegt ist. • DisplayName - Der Anzeigename des Volumes.
public ShadowCopyType ShadowCopyType { get; set; }	Ruft die Art des Kopiervorgangs für die Übertragung ab oder legt diese fest. ShadowCopyType ist eine Aufzählung von Werten. Die folgenden Werte sind verfügbar: • Unknown • Copy • Full

Tabelle 111.

Methode	Beschreibung

public AgentTransferConfiguration TransferConfiguration { get; set; }	Ruft die Übertragungskonfiguration ab oder legt diese fest.
	AgentTransferConfiguration ist ein Objekt mit den folgenden Daten:
	• MaxConcurrentStreams - die maximale Anzahl gleichzeitiger TCP-Verbindungen, die der Core für die Datenübertragung zum Agenten herstellt.
	• MaxTransferQueueDepth - die maximale Anzahl der Blockerweiterungen, die in die Schreibwarteschlange eingereiht werden können.
	• MaxConcurrentWrites - die maximale Anzahl der Blockschreibvorgänge, die zu einem bestimmten Zeitpunkt für eine Epoche ausstehen. Werden weitere Blöcke empfangen, während noch so viele Blockschreibvorgänge ausstehen, werden diese zusätzlichen Blöcke ignoriert, bis einer der ausstehenden Blöcke geschrieben wurde.
	• MaxSegmentSize - maximale Anzahl zusammenhängender Blöcke für die Übertragung einer einzelnen Anforderung.
	• Priority - ein Objekt mit den folgenden Daten:
	  • Undefined
	  • One
	  • Two
	  • Three
	  • Four
	  • Five
	  • Six
	  • Seven
	  • Eight
	  • Nine
	  • Ten
	  • Highest (entspricht One)
	  • Lowest (entspricht Ten)
	  • Default (entspricht Five)
	• MaxRetries - die maximale Anzahl von Wiederholungsversuchen bei einer fehlerhaften Übertragung, bis die Übertragung als fehlgeschlagen angesehen wird.
	• UseDefaultMaxRetries - ein Wert der angibt, dass die Anzahl der Wiederholungen der Standardwert ist.
	• ProviderId - die GUID des VSS-Anbieters, der für Snapshots auf diesem Host verwendet werden soll. Hierfür sollte in der Regel der Standardwert übernommen werden.

Tabelle 111.

Methode	Beschreibung
public AgentTransferConfiguration TransferConfiguration { get; set; } (Forts.)	• ExcludedWriterIds - die VSS-Writer-IDs, die aus diesem Snapshot ausgeschlossen werden sollen. Die Writer-ID wird durch den Namen des Writers bestimmt. Dieser Name dient lediglich zu Dokumentationszwecken und muss nicht exakt mit dem tatsächlichen Namen des Writers übereinstimmen. • TransferDataServerPort - ein Wert, in dem der TCP-Port enthalten ist, über den Verbindungen vom Core für die eigentliche Datenübertragung vom Agenten zum Core hergestellt werden. • SnapshotTimeout - der Zeitraum, für den auf den Abschluss einer VSS-Snapshot-Erstellung gewartet wird, bevor der Vorgang wegen Zeitüberschreitung abgebrochen wird. • TransferTimeout - der Zeitraum, für den auf einen weiteren Core-Kontakt gewartet wird, bevor die Snapshot-Erstellung abgebrochen wird. • NetworkReadTimeout - das Zeitlimit für Netzwerklesevorgänge der jeweiligen Übertragung. • NetworkWriteTimeout - das Zeitlimit für Netzwerkschreibvorgänge der jeweiligen Übertragung. • InitialQueueSize - die anfängliche Größe der Warteschlange für Anforderungen. • MinVolumeFreeSpacePercents - der minimale freie Speicherplatz auf einem Volume Prozent. • MaxChangeLogsSizePercents - die maximale Größe der Protokolle für Treiberänderungen in Bezug auf die Volume-Kapazität in Prozent. • EnableVerification - ein Wert, der angibt, oder für jeden an den Core gesendeten Block eine Diagnoseprüfung durchgeführt werden soll.
public string Key { get; set; }	Die Key-Methode erzeugt einen pseudozufälligen (aber kryptografisch nicht sicheren) Schlüssel, der als einmaliges Kennwort für die Authentifizierung von Übertragungsanforderungen verwendet werden kann.
public bool ForceBaseImage { get; set; }	Ruft den Wert, der angibt, ob die Übertragung eine erzwungene Erfassung eines Basisimage war, ab oder legt diesen fest.
public bool IsLogTruncation { get; set; }	Ruft den Wert, der angibt, ob das Protokoll gekürzt wurde, ab oder legt diesen fest.
public uint LatestEpochSeenByCore { get; set; }	Ruft den letzten Epoch-Wert ab oder legt diesen fest. Die LatestEpochSeenByCore-Methode gibt die Ordnungszahl des zuletzt vom Core erstellten Snapshots zurück. Hierbei handelt es sich um die „Epochennummer“, die dem jeweiligen Snapshot bei der Erstellung mit VSS vom Filtertreiber zugewiesen wurde.

TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Die folgende Tabelle enthält die verfügbaren Objekte für den TransferPostscript-Parameter.

Tabelle 112.

Methode	Beschreibung
public VolumeNameCollection VolumeNames (get; set;)	Ruft die Volume-Namen für die Übertragung ab oder legt diese fest. VolumeNames ist eine Datenstruktur, die die folgenden Daten enthält: • GuidName - Die dem Volume zugeordnete GUID, die als Name verwendet wird, wenn DisplayName nicht festgelegt ist. • DisplayName - Der Anzeigename des Volumes.
public ShadowCopyType ShadowCopyType { get; set; }	Ruft die Art des Kopiervorgangs für die Übertragung ab oder legt diese fest. ShadowCopyType ist eine Aufzählung von Werten. Die folgenden Werte sind verfügbar: • Unknown • Copy • Full

Tabelle 112.

Methode	Beschreibung

public AgentTransferConfiguration TransferConfiguration { get; set; }	Ruft die Übertragungskonfiguration ab oder legt diese fest.
	AgentTransferConfiguration ist ein Objekt mit den folgenden Daten:
	• MaxConcurrentStreams - die maximale Anzahl gleichzeitiger TCP-Verbindungen, die der Core für die Datenübertragung zum Agenten herstellt.
	• MaxTransferQueueDepth - die maximale Anzahl der Blockerweiterungen, die in die Schreibwarteschlange eingereiht werden können.
	• MaxConcurrentWrites - die maximale Anzahl der Blockschreibvorgänge, die zu einem bestimmten Zeitpunkt für eine Epoche ausstehen. Werden weitere Blöcke empfangen, während noch so viele Blockschreibvorgänge ausstehen, werden diese zusätzlichen Blöcke ignoriert, bis einer der ausstehenden Blöcke geschrieben wurde.
	• MaxSegmentSize - maximale Anzahl zusammenhängender Blöcke für die Übertragung einer einzelnen Anforderung.
	• Priority - ein Objekt mit den folgenden Daten:
	  • Undefined
	  • One
	  • Two
	  • Three
	  • Four
	  • Five
	  • Six
	  • Seven
	  • Eight
	  • Nine
	  • Ten
	  • Highest (entspricht One)
	  • Lowest (entspricht Ten)
	  • Default (entspricht Five)
	• MaxRetries - die maximale Anzahl von Wiederholungsversuchen bei einer fehlerhaften Übertragung, bis die Übertragung als fehlgeschlagen angesehen wird.
	• UseDefaultMaxRetries - ein Wert der angibt, dass die Anzahl der Wiederholungen der Standardwert ist.
	• ProviderId - die GUID des VSS-Anbieters, der für Snapshots auf diesem Host verwendet werden soll. Hierfür sollte in der Regel der Standardwert übernommen werden.

Tabelle 112.

Methode	Beschreibung
public AgentTransferConfiguration TransferConfiguration { get; set; } (Forts.)	• ExcludedWriterIds - die VSS-Writer-IDs, die aus diesem Snapshot ausgeschlossen werden sollen. Die Writer-ID wird durch den Namen des Writers bestimmt. Dieser Name dient lediglich zu Dokumentationszwecken und muss nicht exakt mit dem tatsächlichen Namen des Writers übereinstimmen. • TransferDataServerPort - ein Wert, in dem der TCP-Port enthalten ist, über den Verbindungen vom Core für die eigentliche Datenübertragung vom Agenten zum Core hergestellt werden. • SnapshotTimeout - der Zeitraum, für den auf den Abschluss einer VSS-Snapshot-Erstellung gewartet wird, bevor der Vorgang wegen Zeitüberschreitung abgebrochen wird. • TransferTimeout - der Zeitraum, für den auf einen weiteren Core-Kontakt gewartet wird, bevor die Snapshot-Erstellung abgebrochen wird. • NetworkReadTimeout - das Zeitlimit für Netzwerklesevorgänge der jeweiligen Übertragung. • NetworkWriteTimeout - das Zeitlimit für Netzwerkschreibvorgänge der jeweiligen Übertragung. • InitialQueueSize - die anfängliche Größe der Warteschlange für Anforderungen. • MinVolumeFreeSpacePercents - der minimale freie Speicherplatz auf einem Volume Prozent. • MaxChangeLogsSizePercents - die maximale Größe der Protokolle für Treiberänderungen in Bezug auf die Volume-Kapazität in Prozent. • EnableVerification - ein Wert, der angibt, oder für jeden an den Core gesendeten Block eine Diagnoseprüfung durchgeführt werden soll.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Ruft die Speicherkonfiguration ab oder legt diese fest. Das AgentProtectionStorageConfiguration-Objekt enthält die folgenden Daten: • RepositoryId - Name des Repositorys, in dem die Wiederherstellungspunkte des betreffenden Agenten gespeichert werden. • EncryptionKeyId - die ID des Verschlüsselungsschlüssels für die Wiederherstellungspunkte des betreffenden Agenten. Eine leere Zeichenfolge bedeutet keine Verschlüsselung.
public string Key { get; set; }	Die Key-Methode erzeugt einen pseudozufälligen (aber kryptografisch nicht sicheren) Schlüssel, der als einmaliges Kennwort für die Authentifizierung von Übertragungsanforderungen verwendet werden kann.
public bool ForceBaseImage { get; set; }	Ruft den Wert, der angibt, ob die Übertragung eine erzwungene Erfassung eines Basisimage war, ab oder legt diesen fest.
public bool IsLogTruncation { get; set; }	Ruft den Wert, der angibt, ob das Protokoll gekürzt wurde, ab oder legt diesen fest.
public uint LatestEpochSeenByCore { get; set; }	Ruft den letzten Epoch-Wert ab oder legt diesen fest. Die LatestEpochSeenByCore-Methode gibt die Ordnungszahl des zuletzt vom Core erstellten Snapshots zurück. Hierbei handelt es sich um die „Epochennummer“, die dem jeweiligen Snapshot bei der Erstellung mit VSS vom Filtertreiber zugewiesen wurde.

Tabelle 112.

Methode	Beschreibung
public Guid SnapshotSetId { get; set; }	Ruft die GUID ab oder legt diese fest, die diesem Snapshot von VSS zugewiesen wurde.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Ruft die Snapshot-Informationen für jedes Volume, das im Snapshot enthalten ist, ab oder legt diese fest.

VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

Die folgende Tabelle enthält die verfügbaren Objekte für den VirtualMachineLocation-Parameter.

Tabelle 113.

Methode	Beschreibung
public string Description { get; set;}	Ruft eine lesbare Beschreibung dieses Speicherortes ab oder legt diese fest.
public string Method { get; set;}	Ruft den Namen der VM ab oder legt diesen fest.

VolumeImageIdsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

Übernimmt die jeweiligen Werte vom Parameter System.Collections.ObjectModel.Collection<Zeichenfolge>.

VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

Die folgende Tabelle enthält die verfügbaren Objekte für den VolumeName-Parameter.

Tabelle 114.

Methode	Beschreibung
public string GuidName { get; set;}	Ruft die Volume-ID ab oder legt diese fest.
public string DisplayName { get; set;}	Ruft den Volume-Namen ab oder legt diesen fest.
public string UrlEncode()	Ruft eine URL-codierte Version des Namens ab, die problemlos in einer URL übergeben werden kann. **HINWEIS:** In .NET 4.0 WCF ist ein Problem bekannt (https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312), das verhindert , dass Escapezeichen von Pfaden in einer URI-Vorlage richtig funktionieren. Da ein Volume-Name sowohl '\' als auch '?' enthält, müssen Sie die Sonderzeichen '\' und '?' durch andere Sonderzeichen ersetzen.
public string GetMountName()	Gibt einen Namen für dieses Volume zurück, der eine Bereitstellung des Volume-Image in einem Ordner ermöglicht.

VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage)

Übernimmt die jeweiligen Werte vom Parameter System.Collections.ObjectModel.Collection<VolumeName>.

Die folgende Tabelle enthält die verfügbaren Objekte für den VolumeNameCollection-Parameter.

Tabelle 115.

Methode	Beschreibung
public override bool Equals(object obj)	Bestimmt, ob diese Instanz und ein angegebenes Objekt, das auch ein VolumeNameCollection-Objekt sein muss, denselben Wert aufweisen. (Überschreibt Object.Equals(Object).)
public override int GetHashCode()	Gibt den Hashcode für dieses VolumeNameCollection-Objekt aus. (Überschreibt Object.GetHashCode().)

VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer)

Die folgende Tabelle enthält die verfügbaren Objekte für den VolumeSnapshotInfo-Parameter.

Tabelle 116.

Methode	Beschreibung
public Uri BlockHashesUri { get; set;}	Ruft den URI, auf dem die MD5-Hashes von Volume-Blöcken gelesen werden können, ab oder legt diesen fest.
public Uri BlockDataUri { get; set;}	Ruft den URI, auf dem die Volume-Datenblöcke gelesen werden können, ab oder legt diesen fest.

VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer)

Übernimmt die jeweiligen Werte vom Parameter System.Collections.ObjectModel.Collection<VolumeName, VolumeSnapshotInfo>.

Beispiele für PowerShell-Skripts

Die folgenden Beispielskripts werden zur Verfügung gestellt, um die Administratoren bei der Ausführung von PowerShell-Skripts zu unterstützen. Die Beispielskripts umfassen:

- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

PreTransferScript.ps1

Das Skript PreTransferScript wird auf der Agentenseite vor der Übertragung eines Snapshots ausgeführt.

Beispiel: PreTransferScript

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)

# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null

# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];

# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {

     echo 'TransferPrescriptParameterObject parameter is null'
}
else {

     echo
     'TransferConfiguration:'$TransferPrescriptParameterObject.TransferConfiguratio
     n

     echo 'StorageConfiguration:'
     $TransferPrescriptParameterObject.StorageConfiguration
}
```

PostTransferScript.ps1

Das Skript PostTransferScript wird auf der Agentenseite vor der Übertragung eines Snapshots ausgeführt.

Beispiel: PostTransferScript

```
# receiving parameter from transfer job
param([object] $TransferPostscriptParameter)

# building path to Agent's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null

# Converting input parameter into specific object
$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];

# Working with input object. All echo's are logged
```

```
if($TransferPostscriptParameterObject -eq $null) {
      echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
            echo 'ShadowCopyType:' $TransferPostscriptParameterObject.ShadowCopyType
      echo 'ForceBaseImage:' $TransferPostscriptParameterObject.ForceBaseImage
      echo 'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation
}
```

PreExportScript.ps1

Das Skript PreExportScript wird vor einem Exportjob auf der Core-Seite ausgeführt.

Beispiel: PreExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null

# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
      echo 'ExportJobRequestObject parameter is null'
}
else {
      echo 'Location:' $ExportJobRequestObject.Location
      echo 'Priority:' $ExportJobRequestObject.StorageConfiguration
}
```

PostExportScript.ps1

Das Skript PostExportScript wird nach einem Exportjob auf der Core-Seite ausgeführt.

HINWEIS: Es gibt keine Eingabeparameter für PostExportScript, wenn es für die einmalige Ausführung auf dem exportierten Agenten nach der Inbetriebnahme verwendet wurde. Reguläre Agenten sollten dieses Skript im PowerShell-Skriptordner als PostExportScript.ps1 enthalten.

Beispiel: PostExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
```

```
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'

# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {

     echo 'ExportJobRequestObject parameter is null'
}
else {

     echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds

     echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

PreNightlyJobScript.ps1

Das Skript PreNightlyJobScript wird auf der Core-Seite vor jedem nächtlichen Job ausgeführt. Es verfügt über den Parameter $JobClassName, der die getrennte Verarbeitung von untergeordneten Jobs ermöglicht.

Beispiel: PreNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null

# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum
Check Job and Log Truncation Job. All of them are triggering the script, and
$JobClassMethod (contain job name that calls the script) helps to handle those child
jobs separately
switch ($JobClassMethod) {

# working with NightlyAttachability Job
   NightlyAttachabilityJob {

      $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
      [Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];

      echo 'Nightly Attachability job results:';

            if($NightlyAttachabilityJobRequestObject -eq $null) {
```

```
            echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
            echo 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;
            echo 'IsNightlyJob:'
            $NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Rollup Job
  RollupJob {
    $RollupJobRequestObject = $RollupJobRequest -as
    [Replay.Core.Contracts.Rollup.RollupJobRequest];
    echo 'Rollup job results:';
        if($RollupJobRequestObject -eq $null) {
            echo 'RollupJobRequestObject parameter is null';
        }
        else {
            echo 'SimultaneousJobsCount:'
            $RollupJobRequestObject.SimultaneousJobsCount;
            echo 'AgentId:' $RollupJobRequestObject.AgentId;
            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as
        "System.Collections.Generic.List``1[System.Guid]"
        if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
        }
        else {
            echo 'Agents GUIDs:'
            foreach ($a in $AgentsCollection) {
                echo $a
        }
    }
    break;
  }
# working with Checksum Check Job
    ChecksumCheckJob {
        $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
        [Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
        echo 'Exchange checksumcheck job results:';
        if($ChecksumCheckJobRequestObject -eq $null) {
```

```
                echo 'ChecksumCheckJobRequestObject parameter is null';
        }
        else {
                echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
                echo 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
                echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
            }
            break;
        }
# working with Log Truncation Job
   TransferJob {
        $TransferJobRequestObject = $TransferJobRequest -as
        [Replay.Core.Contracts.Transfer.TransferJobRequest];
        echo 'Transfer job results:';
        if($TransferJobRequestObject -eq $null) {
                echo 'TransferJobRequestObject parameter is null';
        }
        else {
                echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
                echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
            }
            echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
            break;
        }
}
```

PostNightlyJobScript.ps1

Das Skript PostNightlyJobScript wird auf der Core-Seite nach jedem nächtlichen Job ausgeführt. Es verfügt über den Parameter $JobClassName, der die getrennte Verarbeitung von untergeordneten Jobs ermöglicht.

Beispiel: PostNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore,
[object]$TakeSnapshotResponse)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
```

```
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2= $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null

# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum
Check Job and Log Truncation Job. All of them are triggering the script, and
$JobClassMethod (contain job name that calls the script) helps to handle those child
jobs separately
switch ($JobClassMethod) {

# working with NightlyAttachability Job
   NightlyAttachabilityJob {

      $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
      [Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];

      echo 'Nightly Attachability job results:';

      if($NightlyAttachabilityJobRequestObject -eq $null) {

            echo 'NightlyAttachabilityJobRequestObject parameter is null';

      }

      else {

            echo 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;

            echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;

      }

      break;
   }

# working with Rollup Job
   RollupJob {

      $RollupJobRequestObject = $RollupJobRequest -as
      [Replay.Core.Contracts.Rollup.RollupJobRequest];

      echo 'Rollup job results:';

      if($RollupJobRequestObject -eq $null) {

            echo 'RollupJobRequestObject parameter is null';

      }

      else {

            echo 'SimultaneousJobsCount:'
            $RollupJobRequestObject.SimultaneousJobsCount;

            echo 'AgentId:' $RollupJobRequestObject.AgentId;

            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;

      }

      $AgentsCollection = $Agents -as
      "System.Collections.Generic.List``1[System.Guid]"

      if($AgentsCollection -eq $null) {

            echo 'AgentsCollection parameter is null';

      }

      else {

      echo 'Agents GUIDs:'

            foreach ($a in $AgentsCollection) {
```

```
                echo $a
                }
            }
            break;
        }
# working with Checksum Check Job
   ChecksumCheckJob {
      $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
      [Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
      echo 'Exchange checksumcheck job results:';
      if($ChecksumCheckJobRequestObject -eq $null) {
            echo 'ChecksumCheckJobRequestObject parameter is null';
      }
      else {
            echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
            echo 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
            echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
      }
      break;
   }
# working with Log Truncation Job
   TransferJob {
      $TransferJobRequestObject = $TransferJobRequest -as
      [Replay.Core.Contracts.Transfer.TransferJobRequest];
      echo 'Transfer job results:';
      if($TransferJobRequestObject -eq $null) {
            echo 'TransferJobRequestObject parameter is null';
      }
      else {
             echo 'TransferConfiguration:'
            $TransferJobRequestObject.TransferConfiguration;
            echo 'StorageConfiguration:'
            $TransferJobRequestObject.StorageConfiguration;
      }
      echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
      $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
      [Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
      if($TakeSnapshotResponseObject -eq $null) {
            echo 'TakeSnapshotResponseObject parameter is null';
      }
      else {
            echo 'ID of this transfer session:' $TakeSnapshotResponseObject.Id;
```

```
            echo 'Volumes:' $TakeSnapshotResponseObject.Volumes;
        }
        break;
    }
}
```

Informationen zum Erstellen von Bourne Shell-Skripts in AppAssure

Die Bourne Shell (sh) oder Bourne Again Shell (BASH) ist ein Shell-Sprach- oder Befehlszeileninterpreter für Unix-basierte Betriebssysteme, der in AppAssure für Linux verwendet wird, um Umgebungen anzupassen und bestimmte Vorgänge in einer vorab festgelegten Reihenfolge auszuführen. Für Bourne Shell-Dateien wird die Dateierweiterung und Namenskonvention .sh verwendet.

Mithilfe der Hooks von Vor- und Nachskripts für Übertragung und Export können Sie vor und nach einer Übertragung oder einem Export Systemvorgänge durchführen. Sie können beispielsweise einen bestimmten cron-Job deaktivieren, während eine Übertragung stattfindet, und nach Abschluss der Übertragung wieder aktivieren. Ein weiteres Beispiel wäre die Notwendigkeit, bestimmte Befehle auszuführen, um anwendungsspezifische Daten auf Festplatte zu speichern. Die Inhalte werden in eine temporäre Datei geschrieben und mit „exec“ ausgeführt. Dadurch wird das Skript mit dem in der ersten Zeile des Skripts angegebenen Interpreters, z. B. (#!/usr/bin/env bash), oder der Standard-Shell ausgeführt, die über die Umgebungsvariable $SHELL festgelegt ist (sofern explizit kein Interpreter im Skript angegeben ist). Sie können in der #!-Zeile des Skripts wahlfrei jeden gewünschten Interpreter einsetzen und verwenden, z. B. zsh, tcsh usw. So können Sie jede andere Shell als die Standard-Shell verwenden.

Sie können verfügbare Objekte des TransferPrescript-Parameters oder eigene Parameter zu den Skripts PreTransferScript.sh und PostTransfer.sh hinzufügen, um die Skripts anzupassen.

Voraussetzungen für Bourne Shell-Skripts

Die Skripts müssen PreTransferScript.sh, PostTransfer.sh und PostExportScript.sh heißen und müssen sich im Verzeichnis /opt/appassure/scripts/ befinden.

Testen von Bourne Shell-Skripts

Sie können die Tests, die ausgeführt werden sollen, mit dem Editor für Skriptdateien (.sh) testen.

HINWEIS: Wenn ein Bourne Shell-Vor- oder Nachskript fehlschlägt, schlägt auch der Job fehl. Informationen zum Job finden Sie in der Datei /var/log/appassure/appassure.log.

Bei erfolgreich ausgeführten Skripts wird der Exit-Code 0 zurückgegeben.

Eingabeparameter für Bourne Shell-Skripts

Die Parameter für die Bourne Shell-Skripterstellung in AppAssure sind in den folgenden Tabellen beschrieben.

TransferPrescriptParameters_VolumeNames

Die folgende Tabelle enthält die verfügbaren Objekte für den TransferPrescript-Parameter.

Tabelle 117.

Methode	Beschreibung
public VolumeNameCollection VolumeNames (get; set;)	Ruft die Volume-Namen für die Übertragung ab oder legt diese fest. VolumeNames ist eine Datenstruktur, die die folgenden Daten enthält: • GuidName - Die dem Volume zugeordnete GUID, die als Name verwendet wird, wenn DisplayName nicht festgelegt ist. • DisplayName - Der Anzeigename des Volumes.
public ShadowCopyType ShadowCopyType { get; set; }	Ruft die Art des Kopiervorgangs für die Übertragung ab oder legt diese fest. ShadowCopyType ist eine Aufzählung von Werten. Die folgenden Werte sind verfügbar: • Unknown • Copy • Full
public string Key { get; set; }	Die Key-Methode erzeugt einen pseudozufälligen (aber kryptografisch nicht sicheren) Schlüssel, der als einmaliges Kennwort für die Authentifizierung von Übertragungsanforderungen verwendet werden kann.
public bool ForceBaseImage { get; set; }	Ruft den Wert, der angibt, ob die Übertragung eine erzwungene Erfassung eines Basisimage war, ab oder legt diesen fest.
public bool IsLogTruncation { get; set; }	Ruft den Wert, der angibt, ob das Protokoll gekürzt wurde, ab oder legt diesen fest.
public uint LatestEpochSeenByCore { get; set; }	Ruft den letzten Epoch-Wert ab oder legt diesen fest. Die LatestEpochSeenByCore-Methode gibt die Ordnungszahl des zuletzt vom Core erstellten Snapshots zurück. Hierbei handelt es sich um die „Epochennummer“, die dem jeweiligen Snapshot bei der Erstellung mit VSS vom Filtertreiber zugewiesen wurde.

TransferPostscriptParameter

Die folgende Tabelle enthält die verfügbaren Objekte für den TransferPostscript-Parameter.

Tabelle 118.

Methode	Beschreibung
public VolumeNameCollection VolumeNames (get; set;)	Ruft die Volume-Namen für die Übertragung ab oder legt diese fest. VolumeNames ist eine Datenstruktur, die die folgenden Daten enthält: • GuidName - Die dem Volume zugeordnete GUID, die als Name verwendet wird, wenn DisplayName nicht festgelegt ist. • DisplayName - Der Anzeigename des Volumes.
public ShadowCopyType ShadowCopyType { get; set; }	Ruft die Art des Kopiervorgangs für die Übertragung ab oder legt diese fest. ShadowCopyType ist eine Aufzählung von Werten. Die folgenden Werte sind verfügbar: • Unknown • Copy • Full

Tabelle 118.

Methode	Beschreibung
public string Key { get; set; }	Die Key-Methode erzeugt einen pseudozufälligen (aber kryptografisch nicht sicheren) Schlüssel, der als einmaliges Kennwort für die Authentifizierung von Übertragungsanforderungen verwendet werden kann.
public bool ForceBaseImage { get; set; }	Ruft den Wert, der angibt, ob die Übertragung eine erzwungene Erfassung eines Basisimage war, ab oder legt diesen fest.
public bool IsLogTruncation { get; set; }	Ruft den Wert, der angibt, ob das Protokoll gekürzt wurde, ab oder legt diesen fest.
public uint LatestEpochSeenByCore { get; set; }	Ruft den letzten Epoch-Wert ab oder legt diesen fest. Die LatestEpochSeenByCore-Methode gibt die Ordnungszahl des zuletzt vom Core erstellten Snapshots zurück. Hierbei handelt es sich um die „Epochennummer“, die dem jeweiligen Snapshot bei der Erstellung mit VSS vom Filtertreiber zugewiesen wurde.

Beispiele für Bourne Shell-Skripts

Die folgenden Beispielskripts werden zur Verfügung gestellt, um die Administratoren bei der Ausführung von Bourne Shell-Skripts zu unterstützen. Sie können die Beispielskripts verwenden und je nach Bedarf anpassen. Die Beispielskripts für Agenten umfassen:

- PreTransferScript.sh
- PostTransferScript.sh
- PostExportScript.sh

HINWEIS: Der Agent startet das Skript mit dem Shell-Befehl „exec“. Sie können den Interpreter für die Skriptausführung in der ersten Zeile des Skripts angeben (ähnlich wie bei der Definition normaler Skripts, die von der Befehlszeile aus durchgeführt werden). Wird kein Interpreter angegeben, wird das Skript von der Standard-Shell interpretiert. Wenn Sie eine andere Shell als die Standard-Shell angeben, müssen Sie sicherstellen, dass der angegebene Interpreter auf allen geschützten Maschinen vorhanden ist.

PreTransferScript.sh

Das Skript PreTransferScript wird auf der Agentenseite vor der Übertragung eines Snapshots ausgeführt.

Das folgende Skript speichert die Werte der Eingabeparameter in der Datei Pre(Post)TransferScriptResult.txt, die im Stammbasisverzeichnis gespeichert ist.

Beispiel: PreTransferScript

```
#!/bin/bash
echo
"TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyTyp
e
TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImag
e
TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncat
ion
TransferPrescriptParameter_LatestEpochSeenByCore=$TransferPrescriptParameter_Latest
EpochSeenByCore" > ~/PreTransferScriptResult.txt
exit 0
```

PostTransferScript.sh

Das Skript PostTransferScript wird auf der Agentenseite vor der Übertragung eines Snapshots ausgeführt.

Das folgende Skript speichert die Werte der Eingabeparameter in der Datei Pre(Post)TransferScriptResult.txt, die im Stammbasisverzeichnis gespeichert ist.

Beispiel: PostTransferScript

```
#!/bin/bash
echo
"TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyT
ype
TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseIm
age
TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTrunc
ation
TransferPostscriptParameter_LatestEpochSeenByCore=$TransferPostscriptParameter_Late
stEpochSeenByCore" > ~/PostTransferScriptResult.txt
exit 0
```

PostExportScript.sh

Das Skript PostExportScript wird nach der Übertragung auf der Agentenseite ausgeführt.

Das folgende Skript speichert die Werte der Eingabeparameter in der Datei Pre(Post)ExportScriptResult.txt, die im Stammbasisverzeichnis gespeichert ist.

Beispiel: PostExportScript

```
#!/bin/bash
echo
"$curr_name-exported" > /etc/hostname
exit 0
```

Glossar

A

Agent

Ein Agent ist eine Maschine bzw. ein Server, die/der durch AppAssure geschützt ist oder geschützt werden soll.

AppAssure

AppAssure setzt neue Standards beim Datenschutz. Dazu werden Sicherung, Replikation und Wiederherstellung in einer Lösung kombiniert, die als extrem schnelle und zuverlässige Sicherungslösung zum Schutz von virtuellen Maschinen (VM) sowie von physischen und Cloud-Umgebungen konzipiert wurde.

Aufbewahrung

Die Aufbewahrung definiert den Zeitraum, für den Sicherungs-Snapshots der geschützten Maschinen im AppAssure Core gespeichert werden. Der Rollup-Prozess sorgt dafür, dass die Aufbewahrungsrichtlinie für die Wiederherstellungspunkte eingehalten wird.

B

Bereitstellbarkeit

Die Exchange-Bereitstellbarkeit ermöglicht die Ermittlung von Beschädigungen. Sie weist Administratoren auf mögliche Fehler hin und stellt sicher, dass alle Daten auf den Exchange-Servern bei einem Ausfall erfolgreich wiederhergestellt werden.

C

Central Management Console

Die AppAssure Central Management Console ist ein Verwaltungsportal für mehrere Cores. Sie vereinfacht die Verwaltung mehrerer Bereitstellungen von AppAssure Cores. Mit der Central Management Console können Sie Bereitstellungen in einer einzelnen, webbasierten Oberfläche gruppieren und verwalten.

Cluster

Siehe Windows-Failover-Cluster.

Cluster-Knoten

Eine einzelne Maschine, die Teil eines Windows-Failover-Clusters ist.

Core

Der AppAssure Core ist die zentrale Komponente der AppAssure-Architektur. Der Core stellt die grundlegenden Dienste für Sicherung, Wiederherstellung, Aufbewahrung, Replikation, Archivierung und Verwaltung bereit. Im Kontext der Replikation wird der Core auch als *Quell-Core* bezeichnet. Der Quell-Core ist der Ursprung und der Ziel-Core ist das Ziel.

D

Datenbankverfügbarkeitsgruppe (DAG)

Eine Gruppe von bis zu 16 Microsoft Exchange Server 2010-Postfachservern, die eine automatische Wiederherstellung auf Datenbankebene bei Datenbank-, Server oder Netzwerkfehlern ermöglicht. DAGs verwenden die kontinuierliche Replikation und einen Teil der Windows-Technologien für Cluster-Failover, um hohe Verfügbarkeit und Ausfallsicherheit von Standorten zu gewährleisten. Die Postfachserver in einer DAG überwachen sich gegenseitig auf Fehler. Wenn ein Postfachserver einer DAG hinzugefügt wird, arbeitet er mit den anderen Servern in der DAG zusammen, um bei Datenbankfehlern eine automatische Wiederherstellung auf Datenbankebene zu ermöglichen.

E

Einzelkopiecluster

Eine Failover-Cluster-Lösung für Speicher, die eine einzelne Kopie einer Speichergruppe im Speicher verwendet, die von den Knoten im Cluster gemeinsam genutzt wird. Dabei handelt es sich um eine von zwei Bereitstellungsmöglichkeiten für Postfachclusterserver, die in Exchange 2007 verfügbar sind.

F

Fortlaufende Clusterreplikation (CCR)

Eine Failover-Cluster-Lösung für nicht freigegebenen Speicher, die eine integrierte, asynchrone Protokollversandtechnologie verwendet, die auf einem zweiten Server in einem Failover-Cluster eine Kopie jeder Speichergruppe erstellt und verwaltet. CCR ist als Lösung für ein oder zwei Rechenzentren ausgelegt, die eine hohe Verfügbarkeit sowie Ausfallsicherheit von Standorten bietet. Dabei handelt es sich um eine von zwei Bereitstellungsmöglichkeiten für Postfachclusterserver, die in Exchange 2007 verfügbar sind.

G

Globale Deduplizierung

Die Storage Networking Industry Association (SNIA) definiert die Datendeduplizierung als das Ersetzen mehrerer Kopien von Daten – auf verschiedenen Granularitätsebenen – durch Verweise auf eine gemeinsame Kopie, um Speicherplatz oder Bandbreite einzusparen. Der Volume-Manager von AppAssure führt die globale Datendeduplizierung in einem logischen Volume durch. Die Granularität der Deduplizierung beträgt 8 KB. Die Deduplizierung in AppAssure ist auf geschützte Maschinen beschränkt, die das gleiche Repository und den gleichen Verschlüsselungsschlüssel verwenden.

K

Komprimierung

Die Storage Networking Industry Association (SNIA) definiert die Komprimierung als Kodierung von Daten, um deren Größe zu reduzieren.

L

Live Recovery

AppAssure Live Recovery ist eine Technologie zur Sofortwiederherstellung für VMs und Server. Sie gewährt nahezu ununterbrochenen Zugriff auf Datenvolumes von virtuellen oder physischen Servern und ermöglicht dadurch die Wiederherstellung kompletter Volumes in extrem kurzer RTO-Zeit und RPO-Zeiten von wenigen Minuten.

Lizenzportal

Das Dell Software-Lizenzportal ist eine Webschnittstelle, die von Benutzern und Partnern zum Registrieren, Herunterladen, Aktivieren und Verwalten von AppAssure-Lizenzen verwendet wird.

Lizenzschlüssel

Der Lizenzschlüssel, den Sie erhalten, wenn Sie sich beim Dell Software-Lizenzportal für ein Konto registrieren, wird für den Zugriff auf das Dell Software-Lizenzportal verwendet. Über das Dell Software-Lizenzportal können Sie den AppAssure Core und die Agenten herunterladen, Lizenzen und Gruppen verwalten, die Gruppenaktivitäten nachverfolgen, Maschinen registrieren, Konten erstellen, Benutzer einladen und Berichte erstellen.

Local Mount Utility

Das Local Mount Utility ist eine herunterladbare Anwendung, mit der Sie einen Wiederherstellungspunkt in einem remote AppAssure Core auf einer beliebigen Maschine bereitstellen können.

Lokale Konsole

Die lokale Konsole ist eine webbasierte Schnittstelle, die eine umfassende Verwaltung des AppAssure Core ermöglicht.

M

Maschine

Eine Maschine – manchmal auch als Agent bezeichnet – ist ein physischer oder virtueller Computer oder Server, der durch den AppAssure Core geschützt ist. Im Kontext der Replikation kann ein Core auch als *Quell-Core* bezeichnet werden.

O

Objektdateisystem

Der skalierbare Objektspeicher von AppAssure ist eine Objektdateisystemkomponente. Alle Datenblöcke, von denen Snapshots abgeleitet werden, werden als Objekte behandelt, die im Objektdateisystem gespeichert, abgerufen, verwaltet und repliziert werden. Das System ist so ausgelegt, dass eine skalierbare E/A-Leistung) zusammen mit globaler Datendeduplizierung, Verschlüsselung und Aufbewahrungsverwaltung bereitgestellt wird. Das Objektdateisystem verfügt über direkte Schnittstellen zu branchenüblichen Speichertechnologien.

P

Passphrase

Eine Passphrase ist ein Schlüssel, der bei der Datenverschlüsselung verwendet wird. Wenn die Passphrase verloren geht, können die Daten nicht wiederhergestellt werden.

PowerShell Scripting

Windows PowerShell ist eine an Microsoft .NET Framework gebundene Umgebung für die Verwaltungsautomatisierung. AppAssure enthält umfassende Client-SDKs für die Erstellung von PowerShell-Skripts, mit denen Administratoren die Verwaltung von AppAssure-Ressourcen automatisieren können, indem Befehle entweder direkt oder über Skripte ausgeführt werden.

Protokollkürzung

Bei der Protokollkürzung werden Protokolldatensätze aus dem Transaktionsprotokoll entfernt. Wenn Sie bei einer SQL Server-Maschine die Kürzung der SQL Server-Protokolle erzwingen, wird der freie Speicherplatz auf dem SQL-Server ermittelt. Wenn Sie bei einer Exchange Server-Maschine die Kürzung der Exchange Server-Protokolle erzwingen, wird dadurch Speicherplatz auf dem Exchange-Server freigegeben.

Prüfsumme

Die Prüfsummenfunktion ermöglicht das Erstellen von Datenblöcken, mit denen unbeabsichtigte, bei der Übertragung oder Speicherung auftretende Fehlern ermittelt werden können.

Q

Quorum

In einem Failover-Cluster ist ein Quorum die Anzahl der Elemente, die online sein müssen, damit ein bestimmter Cluster betriebsfähig bleibt. Die in diesem Kontext relevanten Elemente sind Cluster-Knoten. Dieser Begriff kann auch für Quorum-fähige Ressourcen verwendet werden, die für die Verwaltung der Konfigurationsdaten ausgewählt wurden, die für die Wiederherstellung des Clusters notwendig sind. Diese Daten enthalten Einzelheiten aller Änderungen, die an der Cluster-Datenbank vorgenommen wurden. Im Allgemeinen können andere Cluster-Ressourcen auf die Quorum-Ressource zugreifen, sodass jeder Cluster-Knoten Zugriff auf die aktuellsten Datenbankänderungen hat. Standardmäßig gibt es nur eine Quorum-Ressource pro Server-Cluster. Eine besondere Quorum-Konfiguration (Einstellungen für einen Failover-Cluster) bestimmt den Punkt, an dem zu viele Fehler den Cluster-Betrieb unmöglich machen.

R

Remote-Core

Ein Remote-Core ist ein AppAssure Core, auf den eine Maschine außerhalb des Core über das Local Mount Utility zugreift.

Replikation

Die Replikation ist selbstoptimierend mit einem einzigartigen Read-Match-Write (RMW)-Algorithmus, der eng mit der Deduplizierung verknüpft ist. Sie stellt die Beziehung zwischen Ziel-Core und Quell-Core am selben Standort oder an zwei Standorten mit langsamer Verbindung dar, wobei der Quell-Core die Daten für jeden Agenten einzeln und asynchron an den Ziel- oder Quell-Core überträgt.

Repository

Ein vom AppAssure Core verwaltetes Repository ist ein Ordner, der zum Speichern von Snapshots verwendet wird, die von den geschützten Servern und Maschinen erfasst wurden. Das Repository kann sich auf verschiedenen Speichertechnologien wie Storage Area Network (SAN), direkt angeschlossener Speicher oder Network Attached Storage (NAS) befinden.

Rollback

Bei einem Rollback werden Volumes auf einer Maschine aus Wiederherstellungspunkten wiederhergestellt.

Rollup

Der Rollup-Prozess ist ein internes, nachts durchgeführtes Wartungsverfahren, das durch Komprimieren und Entfernen veralteter Wiederherstellungspunkte für die Einhaltung der Aufbewahrungsrichtlinie sorgt. AppAssure ist das Rollup auf Metadatenvorgänge beschränkt.

S

Seeding

Hierbei handelt es sich um die Erstübertragung von deduplizierten Basisimages und inkrementellen Snapshots von geschützten Agenten bei der Replikation, die sich auf hunderte oder tausende Gigabytes an Daten summieren kann. Die Anfangsreplikation kann auf dem Ziel-Core mithilfe externer Datenträger erledigt werden, was bei umfangreichen Daten oder Standorten mit langsamer Verbindung sinnvoll ist.

Server-Cluster

Siehe Windows-Failover-Cluster.

Smart Agent

Der AppAssure Smart Agent ist auf den Maschinen installiert, die durch den AppAssure Core geschützt werden. Der Smart Agent protokolliert die geänderten Blöcke auf dem Datenträger-Volume und erstellt in einem vordefiniertem Schutzintervall Snapshots der geänderten Blöcke.

Snapshot

Snapshot ist ein in der Branche gebräuchlicher Ausdruck, mit dem die Fähigkeit zur Erfassung und Speicherung des Zustands eines Datenträger-Volumes zu einem bestimmten Zeitpunkt definiert wird, während Anwendungen ausgeführt werden. Der Snapshot ist entscheidend, wenn eine Systemwiederherstellung aufgrund eines Systemausfalls oder -fehlers erforderlich ist. Die AppAssure-Snapshots sind anwendungskonsistent, d. h. dass alle offenen Transaktionen und laufenden Transaktionsprotokolle abgeschlossen und die Cache-Speicher abgelegt werden, bevor der Snapshot erstellt wird. AppAssure verwendet die Microsoft-Volumeschattenkopie-Dienste (VSS), um konsistente Snapshots beim Absturz von Anwendungen zu ermöglichen.

SQL-Anfügbarkeit

SQL-Anfügbarkeit ist ein Test, der im AppAssure Core durchgeführt wird, um sicherzustellen, dass alle SQL-Wiederherstellungspunkte fehlerfrei und im Falle eines Fehlers für die Sicherung verfügbar sind.

T

Transport Layer Security

TLS (Transport Layer Security) ist ein modernes kryptografisches Netzwerkprotokoll, um eine sichere Kommunikation über das Internet zu gewährleisten. Dieses Protokoll, das von der IETF (Internet Engineering Task Force) definiert wurde, ist der Nachfolger von Secure Sockets Layer (SSL). Im Allgemeinen wird weiterhin der Begriff SSL verwendet. Die beiden Protokolle sind jedoch kompatibel (ein TLS-Client kann mit einem SSL-Server kommunizieren).

True Scale

True Scale ist die skalierbare Architektur von AppAssure.

U

Universal Recovery

Die AppAssure Universal Recovery-Technologie bietet uneingeschränkte Flexibilität bei der Wiederherstellung von Maschinen. Sie ermöglicht die Durchführung monolithischer Wiederherstellungen auf und von beliebigen physischen oder virtuellen Plattformen sowie die inkrementelle Aktualisierung von Wiederherstellung auf virtuellen Maschinen von jeder physischen oder virtuellen Quelle aus. Darüber hinaus können Sie mit dieser Technologie auf Anwendungs-, Element- und Objektebene Wiederherstellungen von einzelnen Dateien, Ordnern, E-Mails, Kalenderelementen, Datenbanken und Anwendungen durchführen.

V

Verified Recovery

Mit der Verified Recovery-Technologie werden automatisierte Wiederherstellungstests durchgeführt und Sicherungen überprüft. Sie unterstützt unterschiedliche Dateisysteme und Server.

Verschlüsselung

Daten werden verschlüsselt, damit sie nur für autorisierte Benutzer zugänglich sind, die über den entsprechenden Entschlüsselungsschlüssel verfügen. Die Datenverschlüsselung erfolgt mithilfe des 256-Bit-AES im CBC-Modus (Cipher Block Chaining). Im CBC-Modus wird jeder Datenblock vor der Verschlüsselung eine XOR-Operation mit dem vorherigen verschlüsselten Textblock ausgeführt. Auf diese Weise hängt jeder neue verschlüsselte Textblock von allen vorausgehenden unverschlüsselten Textblöcken ab. Als Initialisierungsvektor wird eine Passphrase verwendet.

Verwaltungsrollen

Die AppAssure Central Management Console umfasst ein neues Konzept für Verwaltungsrollen, mit dem zur Unterstützung einer sicheren und effizienten Delegierung von Verwaltungsaufgaben administrative Zuständigkeiten unter vertrauenswürdigen Daten- und Service-Administratoren aufgeteilt sowie die Steuerung des Zugriffs ermöglicht werden.

Virtual Standby

Virtual Standby ist ein P2V-Prozess (physisch-zu-virtuell), bei dem eine virtuelle Klonmaschine der geschützten Maschine oder des Agenten erstellt wird. Ein Virtual Standby kann mithilfe eines *Ad-hoc*-Exportvorgangs oder eines Exportvorgangs mit *laufender Aktualisierung* erstellt werden. Bei einem Virtual Standby mit *laufender Aktualisierung* wird er nach jedem vom Quellagenten erfassten Snapshot eine inkrementelle Aktualisierung durchgeführt.

Volume-Manager

Der AppAssure-Volume-Manager verwaltet und speichert Objekte und stellt sie anschließend als logisches Volume dar. Er nutzt eine dynamische Pipeline-Architektur, um True Scale-Skalierbarkeit, Parallelität und ein asynchrones E/A-Modell für hohen Durchsatz mit minimaler E/A-Latenz zu liefern.

W

White-Labeling

AppAssure gibt Anbietern von Sicherungs- und Notfallwiederherstellungsdiensten die Möglichkeit, AppAssure ohne Markenaufdruck zu nutzen (White-Labeling) oder mit eigenem Logo zu versehen (Rebranding) und als eigenes Produkt oder als eigenen Dienst zu verkaufen oder zu vertreiben.

Wiederherstellungspunkte

Wiederherstellungspunkte sind eine Sammlung von Snapshots verschiedener Datenträger-Volumes. Zum Beispiel: C:, D: und E:.

Windows-Failover-Cluster

Eine Gruppe unabhängiger Computer, die zusammenarbeiten, um die Verfügbarkeit von Anwendungen und Diensten zu erhöhen. Die geclusterten Server (so genannte Knoten) sind durch physische Kabel und durch Software miteinander verbunden. Wenn einer der Cluster-Knoten ausfällt, übernimmt ein anderer Knoten die Bereitstellung des Dienstes (dieser Prozess ist als Failover bekannt). Benutzer nehmen nur minimale Dienstunterbrechungen wahr. AppAssure unterstützt den Schutz mehrerer verschiedener SQL Server- und Exchange Server-Cluster.

Z

Ziel-Core

Der Ziel-Core, der manchmal auch als *Replikat-Core* bezeichnet wird, ist der AppAssure Core, der die replizierten Daten vom Quell-Core erhält.

Zielreplikat-Maschine

Die Instanz einer geschützten Maschine auf einem Ziel-Core wird Zielagent oder Replikatagent genannt.

Informationen zu Dell

Dell berücksichtigt die Wünsche seiner Kunden und liefert auf der ganzen Welt innovative Technologien, Geschäftslösungen und Dienstleistungen, die anerkannt und geschätzt werden. Weitere Informationen finden Sie unter www.software.dell.com.

Kontakt zu Dell

Technischer Support:
Online-Support

Produktfragen und Vertrieb:
0800 800-78378

E-Mail:
info@software.dell.com

Technische Supportressourcen

Der technische Support steht Kunden, die Dell-Software mit einem gültigen Wartungsvertrag gekauft haben, und Kunden zur Verfügung, die über eine Testversion verfügen. Das Support Portal ist unter http://software.dell.com/support/ erreichbar.

Das Support Portal stellt Selbsthilfetools bereit, mit denen Sie Probleme schnell und eigenständig lösen können – 24 Stunden am Tag, 365 Tage im Jahr. Darüber hinaus ermöglicht das Portal über ein Online-Serviceanforderungssystem auch direkten Zugang zu unseren Produktsupporttechnikern.

Das Portal bietet folgende Möglichkeiten:

- Erstellen, Aktualisieren und Verwalten von Serviceanforderungen (Supportfälle)
- Anzeigen von Knowledge Base-Artikeln
- Erhalten von Produktbenachrichtigungen
- Herunterladen von Software. Testsoftware finden Sie unter Testdownloads.
- Anzeigen von Videos zur Vorgehensweise
- Teilnahme an Communitydiskussionen
- Chatten mit einem Supporttechniker